REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

PLEASE DO NOT RETURN YOUR FORM TO THE ABOVE ORGANIZATION.

1. REPORT DATE *(DD-MM-YYYY)*	2. REPORT TYPE	3. DATES COVERED *(From - To)*
24-10-2011	Final	27 SEP 2010-30 OCT 2011

4. TITLE AND SUBTITLE
Security Operations Curriculum Package
BS in Global Security and Intelligence Studies,
Security Operations Management Track,
BS in Security Operations Management, Model Curriculum
Embry-Riddle Aeronautical University, Prescott , AZ

5a. CONTRACT NUMBER

5b. GRANT NUMBER
N65236-10-1-8403

5c. PROGRAM ELEMENT NUMBER

6. AUTHOR(S)
Jones, Philip J., PHD
Baker, Robert W. , MA

5d. PROJECT NUMBER

5e. TASK NUMBER

5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)
Embry-Riddle Aeronautical University
3700 Willow Creek Road
Prescott, AZ 86301-3270

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)
SPAWARSYSCEN Atlantic
P.O. Box 190022
North Charleston, SC 29419-9022

10. SPONSOR/MONITOR'S ACRONYM(S)

11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
General public availability

13. SUPPLEMENTARY NOTES

14. ABSTRACT
This report details the results of a unique research effort to identify and incorporate the knowledge levels and skills sets needed by entry-level, government security managers into a four-year college degree curriculum. The report details the curriculum and course content for both a new Security Operations Management Track in the established B.S. in Global Security and Intelligence Studies Degree offered at Embry-Riddle Aeronautical University and a model 4 -year college curriculum for a BS degree in Security Operations Management.

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			Robert W. Baker
UC	UC	UC		127	19b. TELEPHONE NUMBER *(Include area code)* 928-777-3938

Security Operations Curriculum Package

- **BS in Global Security and Intelligence Studies, Security Operations Management Track, Embry-Riddle Aeronautical University, Prescott, AZ**

- **BS in Security Operations Management, Model Curriculum**

Office of the Director of National Intelligence
Grant Number: N65236-10-1-8403
Embry- Riddle Aeronautical University,
Prescott. Arizona Date: Oct 24, 2011

Executive Summary

This package presents to the Office of the Director of National Intelligence (ODNI) curricula for two undergraduate degree programs in the field of Security Operations and Management. The package was prepared by the Global Security and Intelligence Studies (GSIS) Program at Embry-Riddle Aeronautical University, Prescott, Arizona Campus, under a grant from the Office of the Director of National Intelligence. The purpose of the grant was to develop a model degree program, available to any interested university that would provide a pool of well-educated and professionally qualified young men and women who could assume entry-level security officer positions in the Intelligence Community. The grant mandated that the model program should be designed to meet or exceed the required knowledge and skill sets identified in the ODNI's ~~"~~Security Operations 2010: Curriculum and Academic Certification Guidelines for Undergraduate Degree Programs in Security Operations, Version 2.0." These Guidelines were thoroughly implemented at the course level in the degree programs provided in this package.

After consultation with representatives of the ODNI, Embry-Riddle decided to provide two degree programs. The first of these is the addition of a new Track to our existing GSIS Program, an undergraduate, Bachelor of Science, degree program that already incorporated in its courses a large part of the ODNI Guideline requirements. Hence it was decided to reconfigure our existing GSIS Program by adding areas mandated by the Guidelines that either were not covered by in our Program, or were insufficiently covered. The result is a new track in the GSIS Program to be called the Security Operations and Management Track. For the most part, the reconfiguration added more courses in management and cyber-security. The model program, the second offering herein, now largely follows our GSIS/Security Operations and Management Track. We feel confident in doing this, given the recognized success of the standard GSIS Program.

The GSIS Program sees as its primary mission the education and training of some of the best of our youth for service in the national security and intelligence communities, where indeed a significant number of our graduates already serve. We are very pleased to have had the opportunity to work with the ODNI on this grant. The leaders of Embry-Riddle Aeronautical University and our Prescott campus are committed to bringing the new Security Operations and Management Track to ERAU, Prescott. This academic year the GSIS Program is already teaching two of the new courses, and we are confident the new track will be fully implemented in the Fall of 2012. We look forward to working with the ODNI to constantly improve our educational offerings and to placing our graduates in this critically important area of service to the nation. We very much appreciate the assurances of on-going support offered by officials of the ODNI as we move to fully implement our GSIS/Security Operations and Management Track.

Table of Contents

APPENDICES:

1. Introduction:

The objective of this Office of the Director of National Intelligence (ODNI) grant was to develop a 4-year academic bachelor degree program in security operations to provide a well-educated and professionally qualified men and women who could assume future entry-level security officer positions throughout the intelligence community and federal security organizations. The degree program was to be designed to meet or exceed the required knowledge levels and skill sets identified in ODNI's "Security Operations 2010: Curriculum and Academic Certification Guidelines for Undergraduate Degree Programs in Security Operations, Version 2.0 "that was developed by subject matter experts in security, education and intelligence. After development of the curricula for these unique pilot programs, ODNI hopes that other colleges and universities will establish similar degree programs based on the model curriculum and that the graduates of all such programs will increase the quality and quantity of qualified applicants seeking employment with the federal government intelligence and security agencies unique pilot degree programs.

Embry-Riddle Aeronautical University was one of the universities chosen to develop the new curriculum based on the previous experience in developing a successful degree program in Global Security and Intelligence Studies (GSIS) that already incorporated nearly all of the knowledge and skill sets desired. Thus our approach to developing the model security operations degree program was twofold. First, we would perform a gap analysis on our existing GSIS program and the 2010 Security Guidelines, identify and develop any additional courses needed to meet or exceed the 210 requirements and develop a new track in our existing GSIS degree program incorporating these new courses. We have done so and the new degree program is entitled, Global Security and Intelligence Studies, Security Operations Management Track. Students who graduate from this degree program will receive a BS in Global Security and Intelligence Studies and we have mastered all of the knowledge and skill sets identified by the ODNI in their 2010 document. Secondly, we adapted our new GSIS Security Operations Management curriculum into a generic model 4-year degree curriculum leading to a BS in Security Operations Management. These two Security Operations Degree Programs were developed under ODNI Grant Number N65236-10-1-8403.

This curriculum package contains both sets of curriculum and supporting lesson plans for the required specialty courses so that the reader may review our existing successful degree program with the new Security Operations Track and the generic model curriculum that we suggest for creating a security operations degree program. Hopefully, these two curricula and the supporting documents will encourage more colleges and universities to develop academic degree programs in this key profession.

2. **Bachelor of Science in Global Security Intelligence Studies with a Security Operations Management Track Curriculum offered at ERAU, Prescott, Arizona Campus.**

Our Bachelor of Science, Global Security and Intelligence Studies (GSIS) Security Operations Management Track totals (122 hours). Our degree program includes 12 credit hours in a foreign language and 12 credit hours in computer security. The security operations management track was added to ensure that are graduates meet or exceed the knowledge and skill sets for entry level security officers /managers desired by the Office of the Director of National Intelligence, federal law enforcement agencies, state law enforcement and intelligence organizations.

GSIS Degree Program with Security Operations Track

Course Categories	**Credit Hours**
General Education	37
Foreign Language (Not Chinese Track)	12
GSIS Core Courses	37
Senior Project	3
Security Operations Specialty Courses	33
Total Degree Credit Hours	122

General Education

COM 122	English Composition and Literature	3
COM 219	Speech	3
COM 223	Intelligence Writing	3
HU140 -146	Humanities & Arts	3
HU/SS/RS	Elective (upper Level)	3
CS 118	Fundamentals of Computer Programming	3
AES111/ 112	Plant or Animal Biology with laboratory	4
PS XXX	Physical Science Elective	3
PSY 101	Introduction to Psychology	3
SS110	World History	3
MA 140	College Algebra	3
MA 222	Business Statistics	3
Total Credit Hours		37

Foreign Language Requirement

A minimum of twelve credits in a foreign language are required for degree completion. All credits must in the same language. Currently, Chinese, Arabic, and Spanish language instruction is regularly offered on the Prescott Campus. Foreign language credits may be transferred from other accredited institutions towards meeting this requirement.

1XX	Foreign Language	3
2XX	Foreign Language	3
3XX	Foreign Language	3
4XX	Foreign Language	3
Total Credit Hours		12

GSIS Core Courses

BA 201	Principles of Management	3
EC 210	Microeconomics	3
SIS 100	Introduction to Global Security & Intelligence Studies	3
SIS 200	Introduction to the U.S. Legal System	3
SIS 260	Forensic Science Applications in Security and Intelligence	4
SS 204	Introduction to Geography	3
SIS 315	Studies in Global Intelligence I	3
SIS 325	History of Terrorism	3
SS 312	Personality and Profiling	3
SS 320	Government of the United States	3
SS 327	International Relations	3
SS 340	U.S. Foreign Policy	3
Total Credit Hours		37

Senior Project

SIS 4XX	Security Operations Management Practicum	3
Total Credit Hours		3

Security Operations Specialty Courses

CS 2XX	Introduction to Computer Networks	3
SIS2XX	Security Fundamentals	3
SIS 3XX	Security Investigations and Interview Techniques	3
CS 3XX	Introduction to Computer Forensics	3
BA 3XX	Government Acquisitions and Contracting	3
SIS 335	Counterintelligence	3
SIS 422	Homeland Security & Technologies	3
SIS 4XX	Physical Security and Facility Design	3
SIS 4XX	Government Security Operations and Management	3
SIS 410	Corporate Security Operations and Management	-
	or BA 308 Public Administration	3
SIS 425	Information Protection and Computer Security	3
Total Credit Hours		33

GSIS Security Operations Management Track Credits Hours 122

3. Suggested Course of Study -GSIS Security Operations Management Track

Freshman Year

COM 122	English Composition	3
COM 219	Speech	3
MA 140	College Algebra	3
HU140-146	Humanities & Arts	3
AES111/ 112	Plant or Animal Biology with laboratory	4
PSY 101	Introduction to Psychology	3
SS110	World History	3
CS 118	Introductions to Computer Programming	3
PS XXX	Physical Science Elective	3
SS 204	Introduction to Geography	3
Total Credit Hours		32

Sophomore Year

COM 223	Intelligence Writing	3
MA 222	Business Statistics	3
BA201	Principles of Management	3
SIS2XX	Security Fundamentals	3
XXXX	Foreign Language (I &II)	6
EC 210	Microeconomics	3
SIS 260	Forensic Science Applications and Security and Intelligence	4
SIS 100	Introduction to Global Security and Intelligence Studies	3
SIS 200	Introduction to the U.S. Legal System	3
Total Credit Hours		31

Junior Year

CS 2XX	Introduction to Computer Networks	3
HU/SS/RS	Elective (upper Level)	3
XXXX	Foreign Language (III &IV)	6
SIS 325	History of Terrorism	3
SS 312	Personality and Profiling	3
SIS 315	Studies in Global Intelligence I	3
SS 320	Government of the United States	3
SIS 410	Corporate Security Management and Operations or BA 308 Public Administration	- 3
SS 327	International Relations	3
SS 340	U.S. Foreign Policy	3
Total Credit Hours		33

Senior Year

CS 3XX	Introduction to Computer Forensics	3
SIS3XX	Security Investigations and Interview Techniques	3
SIS4XX	Physical Security and Facility Design	3
BA XXX	Government Acquisitions and Contracting	3
SIS335	Counterintelligence	3
SIS 4XX	Government Security Operations and Management	3
SIS 425	Information Protection and Computer Security	3
SIS 4XX	Security Operations Management Practicum	3
SIS 422	Homeland Security and Technologies	3
Total Credit Hours		27

Total Credit Hours BS GSIS, Security Operations Track 122

4. Model Bachelor of Science in Security Operations Management Curriculum

Introduction: Embry-Riddle Aeronautical University developed this model curriculum for a four year bachelor level degree in Security Operations Management under a grant from Office of the Director of National Intelligence (ODNI). The ODNI funded this effort based on their growing need for college educated persons as entry-level security managers in the government and private sectors. Therefore, the model curriculum developed drew heavily on the ODNI occupational research entitled –Security Operations 2010: Curriculum and Academic Certification Guidelines for Undergraduate Degree Programs in Security Operations, Version 2.0. The Guidelines stress the need for the student to have a solid foundation in general education, advanced academic capabilities for security operations and discipline specific knowledge and skills. The goal of the grant was to develop a model curriculum that could be used wholly or in part by a college or university to establish a degree program in this field that is growing and vital area of study to national security.

D*e*gree Course Requirements	**Credit Hours**
General Education Course	46
Advanced Academic Capabilities for Security Operations Courses	40
Discipline Specific Courses -Security Operations Specialty Courses	36
Total Degree Credit Hours	**122**

Note: Recommended Foreign Language Requirement Option described at the end of this curriculum outline.

General Education Courses		**Credit Hours**
100	English Composition and Literature	3
100	Introduction to Psychology	3
100	World History	3
100	Introduction to Geography	3
100	College Algebra	3
100	Business Statistics	3
100	Animal or Plant Biology with laboratory	4
100-200	Humanities & Arts Elective (lower level)	3
100-200	Physical Science Elective	3
200	Speech	3
200	Business Communication or Intelligence Writing	3
200	Introduction to Computer Programming	3
200	Speech	3
200	Microeconomics	3
300-400	Humanities & Arts Elective (upper Level)	3
Total Credits		**46**

Advanced Academic Capabilities for Security Operations Courses

Level	Course Title	Credit Hours
100	Introduction to the Security Profession	3
200	Principles of Management	3
200	Introduction to the U.S. Legal System	3
200	Introduction to Forensic Science Applications (laboratory)	4
200	Introduction to Computer Networks	3
200	Security Fundamentals	3
300	Upper Level Elective Course	6
300	History of Terrorism	3
300	Personality and Profiling	3
300	Government of the United States	3
300	International Relations	3
300	Public Administration	3
Total Credits		40

Note: *Courses in business, psychology, history or security-related courses are recommended as electives to enhance this program.*

Discipline Specific Courses -Security Operations Specialty Courses

Level	Course Title	Credit Hours
300	Security Investigations and Interview Techniques	3
300	Introduction to Computer Forensics	3
300	Counterintelligence	3
400	Homeland Security & Technologies	3
400	Physical Security and Facility Design	3
400	Government Acquisitions and Contracting	3
400	Government Security Operations and Management	3
400	Corporate Security Operations and Management	3
400	Information and Computer Security	3
400	Aviation Security and Technologies	3
400	Emergency Management	3
400	Security Operations Management Practicum	3
Total Credits	Security Specialty Courses	36

Security Operations Management Degree **Total Credits** **122**

Optional Foreign Language Requirement

This optional requirement is highly recommended considering the international nature of business and government now and in the future. If this option is chosen, the college or university will need to drop four courses. We recommend public administration, aviation Security and technologies and emergency management and the one upper level course (a total of 12 credit hours). A minimum of twelve credits in a foreign language in the same foreign language should be included in the degree program. We recommend Spanish, Chinese and Arabic as they are all languages in high demand. Foreign language credits may be transferred from other accredited institutions towards meeting this requirement.

100	Foreign Language	3
200	Foreign Language	3
300	Foreign Language	3
400	Foreign Language	3
Total Credits		12

5.0 Suggested Course of Study Model BS Security Operations Management Degree

Level	Freshman Year	Credit Hours
100	English Composition and Literature	3
200	Speech	3
100	College Algebra	3
100	Humanities & Arts	3
100	Plant or Animal Biology with laboratory	4
100	Introduction to Psychology	3
100	World History	3
100	Introduction to Computer Programming	3
100	Physical Science Elective	3
200	Introduction to Geography	3
Total Credit Hours		31

Level	Sophomore Year	Credit Hours
100	Introduction to the Security Profession	3
200	Professional or Technical Writing	3
200	Business Statistics	3
200	Principles of Management	3
200	Security Fundamentals	3
200	Microeconomics	3
200	Forensic Science Applications and Security and Intelligence	4
200	Introduction to the U.S. Legal System	3
200	Introduction to Computer Networks	3
Total Credit Hours		31

Junior Year		
300	Elective Courses (upper Level)	6
300	Humanities and Arts (Upper level)	3
300	History of Terrorism	3
300	Personality and Profiling	3
300	Government of the United States	3
300	U.S. Foreign Policy	3
300	Corporate Security Management and Operations	3
300	Public Administration	3
300	International Relations	3
300	Introduction to Computer Forensics	3
300	Security Investigations and Interview Techniques	3
Total Credit Hours		33

Senior Year

300	Physical Security and Facility Design	3
300	Government Acquisitions and Contracting	3
300	Counterintelligence	3
400	Government Security Operations and Management	3
400	Information Protection and Computer Security	3
400	Aviation Security	3
400	Introduction to Emergency Management	3
400	Homeland Security and Technologies	3
400	Security Operations Management Practicum	3
Total Credit Hours		27

Total Credit Hours BS, Security Operations Management 122

6.0 Security Operations Management Studies Information and Resources

The introduction and development on a new degree program is a very demanding task especially when the degree goal is to graduate a student with a sound liberal arts background and entry-level professional knowledge and skill sets. This type of a degree program requires a unique blending of academic and professional knowledge coupled with critical thinking skills and practical application ability.

The establishment of a four-year bachelor degree program in Security Operations Management is particularly difficult due to the multidisciplinary nature of the security management profession and the unique government and private organizations that the security professional serves.

Another issue is to identify qualified faculty who have both the academic and professional experience to teach the advanced academic and discipline specific courses necessary for a student to acquire the knowledge and skills sets to succeed in the security operation management profession.

For informational purposes, we would like to offer the following guidance and support to other universities interested in implementing a model security operations and management degree. This guidance is based on our academic and professional experience, professional and educational literature and the ODNI subject matter expertise.

General Guidance and Support Information:

Embry-Riddle Aeronautical University, Prescott, Arizona

The Global Security and Intelligence Studies Faculty will be happy to assist you in developing your initial security operations management program. We believe we are uniquely qualified to provide such assistance, having successfully launched a similar program (the Global Security and Intelligence Studies Degree Program, started in 2003), expanded this program to meet addition ODNI requirements, and drafted the ODNI model curriculum. Please do not hesitate to contact either of us for assistance.

Dr. Philip Jones, Professor, Chairman, Global Studies Department
Email: jonephil@erau.edu Telephone: 928-777-0992

Mr. Robert W. Baker, Associate Professor, Program Chairman, GSIS Program

Email: Robert.W.Baker@erau.edu Telephone: 928-777-3938

You may also wish to visit our program website at:
http://prescott.erau.edu/degrees/undergraduate/global-security-intelligence-studies/

Professional and Academic Resources on Security Operations:

Publications:

1. *Security Operations 2010; Curriculum and Academic Certification Guidelines for Undergraduate Degree Programs in Security Operations, Version 2,* Office of the Director of National Intelligence , Special Security Center, (undated).
2. *Intelligence as a Career: Is It Right For You AND Are You Right For It*., Association of Former Intelligence Officers, (2009)
3. *Career Opportunities in Security, ASIS International, 2005*

Websites

http://www.asisonline.org/about/history/index.xml

ASIS International is the largest and best known organization for security professionals. Their member services include security educational programs, professional reference library resources, employment opportunities, and subject matter experts in all types of security.

https://www.classmgmt.com/About/

NCMS, The Society of Security Professionals is a professional association focusing on government security practices as they relate to the National Industrial Security Program and fostering the highest qualities of security professionalism among its members.

Videos

1. *American Justice, Profiles of Evil: Inside the Criminal Mind,* 50 minutes, Documentary # AAE-73226, A & E , AE Television Network .
2. Criminals in Cyberspace, 50 minutes, Documentary # AAE-72653, A & E , AE Television Network
3. The FBI: A Revealing Inside Look at the Bureau, G75039, 50 minutes, National Geographic
4. FBI‘s Crime Lab ,50 minutes, The History Channel , Documentary # AAE74745 , A & E , AE Television Network
5. Forensic Science: The Crime Fighter‘s Weapon, ,50 minutes, Modern Marvels T, Documentary # AAE72323 , A & E , AE Television Network
6. Investigative Reports, Border Patrol, America‘s Gatekeepers, 50 minutes, Documentary # AAAE113890, A & E , AE Television Network .
7. Investigative Reports: Criminal Evidence, 50 minutes, Documentary # AAE73478, A & E, AE Television Network .
8. Investigative Reports: FEMA in the Face of Disaster , 50 minutes, Documentary # AAE74212 , A & E , AE Television Network

9. Investigative Reports: Violence in the Workplace , 50 minutes, Documentary # AAE18122 , A & E , AE Television Network
10. Post Mortem; The Death Investigation Crisis in America, Frontline , FRL62907, 60 minutes, Public Broadcast Service
11. The 911 Commission Report ,100 minutes, The History Channel , Documentary # AAE71739 , A & E , AE Television Network
12. The Confessions, Frontline , FRL62907, 60 minutes, Public Broadcast Service
13. The Hunt; Fingerprinting and Ballistics, 50 minutes, Documentary # AAE74993 , A & E , AE Television Network
14. The Storm, Frontline , FRL62403, 60 minutes, Public Broadcast Service
15. Terror Tech: Defending the High Rise Forensic Science,50 minutes, Modern Marvels, Documentary # AAE43791 , A & E , AE Television Network
16. Traitors Within, 100 minutes, The History Channel, , Documentary # AAE72459 , A & E , AE Television Network
17. *WikiSecrets,* Frontline , FRL62915, 60 minutes, Public Broadcast Service

.

Appendix 1-1 General Education Course Descriptions

While the general content of these courses is similar, the syllabi and specific lesson plans will often vary with the college or university and instructor preference. Thus we are providing the description of the courses that should form the general education foundation for these degree programs.

COM 122 English Composition and Literature 3 Credits
This course focuses on principles of writing in response to readings in the humanities, social sciences, and other interdisciplinary fields. Students develop their communicative, evaluative, critical thinking, and research writing abilities through the close examination of key texts across those disciplines.

COM 219 Speech 3 Credits
A continuation of the study of communication and communication theory with emphasis on overcoming communication apprehension, developing listening skills, mastering oral performance, and writing about communication. Individual sections may focus on public speaking, group discussion, oral interpretation, or interpersonal communication. Section emphasis varies by instructor and is listed in the Schedule of Courses.

COM 222 Business Communication 3 Credits
An introduction to effective business communication. Topics in oral, written, nonverbal, and intercultural communication are covered. Research methods, effective speaking, and the preparation of letters, memoranda, and reports are emphasized

HU 143 Introduction to Rhetoric 3 Credits
A continuation of COM 122, HU 142 offers a broad survey of rhetorical theory and practice. Whether noble or base, rhetoric primarily uses language to achieve a desired end, usually persuasion. This course employs primary and secondary readings as a means to examine how rhetorical principles manifest themselves in a variety of cultural texts and to understand the powers of persuasion. Although instructors may choose various approaches to teaching this course, students should expect some exposure to classical rhetoricians.

HU 375 The Nature of Language 3 Credits
This course provides a practical investigation into how people use language functions as a system of meaning. The diversity, complexity, and intrinsic fascination of this most human of behaviors is studied largely with reference to the English language. Topics include popular ideas about language, language and identity, language structure and system, language media, language acquisition and learning, language and the brain, and world languages.

AES 111 Plant Biology 4 Credits
This course will study the principles and processes associated with the biology of plants, including a survey of fungi, green Protista, and plants. Major emphasis on vascular

plants, evolutionary origins, and ecological adaptations. One three-hour laboratory session per week.

MA 140 College Algebra 3 Credits
Fundamentals of exponents, radicals, linear, quadratic, and absolute value equations, inequalities, and complex numbers. Introduction to functions, curve sketching, elementary theory of equations, sequences and issues, matrix algebra, and systems of equations**.**

MA 222 Business Statistics 3 Credits
Measures of central tendency and dispersion; histograms; algebra of probability; sample spaces; dependent events; Bayes'Therom with applications; binomial, Poisson, normal distributions, and their relationships; sampling distributions; hypothesis testing; confidence intervals.

PS 113 Introductory Physics I 3 Credits
Survey course in elementary physics. Stress will be placed on basic physics principles. Problem solving and problem solving logic will be an important, integral part of this course. Topics will include Newton's Laws, projectile motion, circular motion, work, energy, conservation laws, and momentum.

PSY 101 Introduction to Psychology 3 Credits
A survey of the bio psychosocial continuum and the intrapsychic, interpersonal, and organization factors affecting human behavior. A primary feature of the course is its focus on the scientific method as the route to psychological knowledge. Students study the rationalist, empiricist, and experimental foundations of the scientific method and how these foundations can be critiqued. Topics include sensation, perception, learning, memory, personality, psychopathology, physiological psychology, and social processes. Emphasis is placed on the application of the basic principles of psychology to engineering, aviation, public policy, and business.

SS 110 World History 3 Credits
Designed primarily as a survey of the development and evolution of Western civilization from 1500 to the present. Emphasis is placed on the effect of Western influence on the world.

SS 204 Introduction to Geography 3 Credits
A survey course designed to acquaint the student with types of maps, map reading and use, as well as to show relationships between geography and economics, culture, and geopolitics. Humans and their use of their environment are stressed, along with the usual emphasis on places, names, and location. Ancillary topics will include climate, demography, and transportation.

EC 210 **Microeconomics** **3 Credits**

An introduction to the economic principles of free enterprise supply and demand, private and social implications of profit maximization, market structure, and resource markets. Current microeconomic issues in aviation (such as liability reform, evolution of airline competition, etc.) are discussed.

Appendix 1-2 Advanced Academic Capabilities for Security Operations Courses
These courses will provide the knowledge levels and the general skill sets needed to be successful in the security operation management profession. The course descriptions are provided except when the course content is considered to be too specialized to be taught at most colleges or universities. In that case, a proposed lesson plan has also been included, denoted by **LP** below

Note: Courses are labeled **A, B** or **AB** denoting whether they are applicable to the GSIS Security Operations Management Curriculum -**A,** the Model Security Operations Management Curriculum- **B** or both degree programs- **AB.**

SIS 100 Introduction to Global Security and Intelligence Studies 3 Credits
SIS 100 is the introductory course for the Global Security and Intelligence Studies program. It discusses the whole range of contemporary international issues, from questions of realism versus idealism in foreign affairs, to changes in the nation-state, the implications of climate change, the proliferation of weapons of mass destruction, international development, the rise of China, and international public health. The course requires the student to closely follow breaking international developments and learn to discuss these objectively and analytically. An important emphasis throughout the course is for the student to learn and demonstrate critical thinking and imagination. **A, LP**

SIS 1XX Introduction to the Security Profession 3 Credits

This introductory course provides students with a familiarity with the general security profession in the government and private organizations. The students will become familiar with general duties and responsibilities of a security profession and vital role they play in protecting people, facilities, and sensitive information. They will also explore the many different areas of specialized security such as government, banking, hospital and school security. During the course, they will be exposed to security professionals in various areas through guest lectures and visits to protected facilities. **B, LP**

SIS 200 Introduction to the US Legal System 3 Credits
This course will provide a general overview of the legal system in the U.S. It is a core course for the GSIS program, designed to give the student a foundation in legal theory and philosophy, the sources of law, the place of the judicial system in the U.S., the structure of the courts, original through appellate jurisdiction, judicial review, the role of the legal profession, the structure of civil and criminal cases, the adversarial process, constitutional law and protections, and the application of law to security and intelligence issues. **AB**

SIS 295 Intelligence Writing 3 Credits
The purpose of this course is to teach the basic skills of intelligence writing. The most essential principle of intelligence writing is to communicate to the reader exactly the message the analyst wants to communicate. Clarity, precision, accuracy, and brevity are key elements of intelligence writing, but also crucial is the overall structure of the intelligence brief. Two further elements are part of the intelligence writing process: a capacity to accurately evaluate information and an ability to make analytical judgments about the significance of a development. All these elements will be covered intensively as part of the intelligence writing process. **A ,LP**

SIS 260 Forensic Science Applications in Security and Intelligence 4 Credits
During this course students will learn the basic scientific principles and concepts underlying the use of forensic science in law enforcement, security, and intelligence. Students will become familiar with the various forensic techniques and their application in real-life situations. They will accomplish these learning objectives through a combination of academic work, practical field applications, and laboratory studies. The course material will focus on the available scientific equipment and tests employed in forensic science and their practical applications in criminal justice, civil proceedings, identification and intelligence analysis and confirmation. The students will learn the methodology employed in preserving a crime scene, collecting physical evidence, transporting and storing such evidence. The students will also review the various biological and chemical tests that could be employed to examine such evidence including their individual applicability, cost and validity. The course will also address the legal issues arising from the use of existing and evolving forensic science techniques in legal proceedings. Throughout the course, students will discuss the professional, legal, and ethical issues surrounding forensic science applications in law enforcement, security, and intelligence applications. **A,B ,LP**

CS 118 Fundamentals of Computer Programming 3 Credits
This course provides the basic concepts of structured programming with applications in business, technology, and engineering. This course is intended for the student with little or no experience in programming. **AB**

SIS 315 Studies in Global Intelligence I 3 Credits
This course will examine the uses of strategic intelligence by world leaders in shaping policy and the effects of strategic intelligence on world events. Issues to be covered include theoretical models of strategic intelligence; intelligence collection, evaluation, analysis, production, and dissemination; intelligence oversight; covert and clandestine operations; intelligence bureaucracies; ethical and moral issues in intelligence; counterintelligence. The course emphasizes strategic intelligence in the business, political, military, scientific, and technological domains. **A,LP**

SIS 325 History of Terrorism 3 Credits
This course will introduce the student to the history of terrorism, from the 19th century up to the present day. It will evaluate the causes of terrorism, the capabilities and limitations of terrorist groups, the requisites of effective counterterrorism responses, and the future prospects of terrorism. It will address the implications of terrorism and asymmetrical warfare for U.S.

national security, including the possible use of weapons of mass destruction. The constitutional and legal implications of counterterrorist strategies will also be discussed. It will examine the organization, objectives, and methodologies of key terrorist groups operating in the 21st century, particularly those showing ideological hardening, religious revivalism, and ethnic militancy. **AB, LP**

SS 312 Personality and Profiling 3 Credits
This course provides a rigorous and comprehensive foundation for explaining, understanding, predicting, and influencing people. This foundation will be applied to stopping people from violating trust – namely, committing espionage – and to identifying and controlling them as quickly as possible after they have violated trust. The course will largely focus on personality theory and research based on scientific methodologies. The course also will explore other approaches to human knowledge and meaning including the philosophy of epistemology, literary criticism, and the interpretation of cultural products such as film, music, dance, and painting. By course's end, students will have profiled a U.S. citizen convicted of spying against his country. **AB, LP**

SS 320 Government of the United States 3 Credits
Basic issues of democracy in the U.S., constitutional principles, and the executive, legislative, and judicial branches of government. **AB**

SS 327 International Relations 3 Credits
This course will examine historical and contemporary themes in international relations that set the stage for analyzing the current and future international system. Toward this, the curriculum is designed to introduce the student to the theory and practice of international relations with the objective of enabling a greater understanding of the global context that shapes issues and outcomes in world affairs. Extending beyond simple description, the student will develop an analytic and anticipatory capacity in which to explain foreign policy and international politics. **AB**

Advanced Academic Capabilities for Security Operations Courses with Syllabus and Lesson Plans

Course Number: SIS 1XX **Credit Hours: 3**

Title: Introduction to the Security Profession

Required Texts:

1. Fisher, Halibozack and Walters, Introduction to Security, *8nd Edition.* Butterworth & Heinemann ,Sebastopol, CA, USA : (2008)
2. *Intelligence as a Career: Is It Right For You AND Are You Right For It*., Association of Former Intelligence Officers, (2009)
3. *Career Opportunities in Security,* ASIS International, 2005
4. *Security Management Magazines,* ASIS International, 2011-12

Supplementary Material:

Position Classification Standard for Security Administration Series, GS -0080, U.S. Office of Personnel Management (December, 1987)

Course Description: This introductory course provides students with a familiarity with the general security profession in the government and private organizations. The students will become familiar with general duties and responsibilities of a security profession and vital role they play in protecting people, facilities, and sensitive information. They will also explore the many different areas of specialized security such as government, banking, hospital and school security. During the course, they will be exposed to security professionals in various areas through guest lectures and visits to protected facilities.

Goals: The goal of this course is to provide the student with a general understanding of the duties and responsibilities of a security professional in both the government and private sector. The student will become aware of the many different technical and management aspects of the security profession in practice. Finally, the students will learn of the many different general and specialized employment opportunities this profession offers domestically and internationally.

Learning Outcomes:

1. Understand the general nature functions of a security profession

2. Be familiar with the general duties and responsibilities of a security professional

3. Be aware of the personal and professional legal and ethical standards expected of those in the security profession

4. Be familiar with basic security functions protection of people, facilities and sensitive security information

5. Gain insight into the profession from professional guest lectures and through visits to protected facilities.

6. Practice professional writing and briefing

Description of Assessment Activities:

Quiz 1-This quiz will assess the student‘s knowledge and understanding of the security profession, legal and ethical behavior required, occupational diversity, etc.

Quiz2 This quiz will assess the student‘s knowledge and understanding of the security profession by building on the information that they have obtained during the first third of the course and the knowledge and skill sets they developed since then.

Quiz 3 This comprehensive quiz will assess the student‘s knowledge and understanding of the security profession, legal and ethical behavior required, specialized security areas, critical thinking and decision making abilities.

Class Activities:

Class Field Trips- The students will take a minimum of one field trip to a protected government or private facility, be briefed by the security manager, tour the facilities and observe security practices and equipment and security

Guest Lecturers: The students will be briefed by security managers who work in specialized area including law enforcement on their daily activities and responsibilities. The students will have the opportunity to talk face-to-face with security professional and discuss the profession‘s benefits and drawbacks with them.

Team Exercise 1 – Student teams will be given a typical security scenario or problem to workout. They will present their solution and decision making process for critique and feedback.

Student Exercise 1 – Select and research a security position in the government or private sector. Determine the qualifications for the position, the job description, the application process, salary and benefit information. Is the position domestic or international and does it require extensive travel, domestic or international. Prepare a summary paper on the position in the format provided by the instructor. Prepare a power point presentation for class presentation. The power point should have 4-8 slides.

Student Exercise 2 –Draft a cover letter and resume for a security position that they have identified as being of interest to them. The student will answer specific questions on their knowledge and skill sets if the job application requires that information.

The student will brief the class on the job he was seeking and the application process.

Scoring and Grading Matrix

Scoring Area	Maximum Points
Quiz 1	50
Quiz 2	50
Quiz 3	50
Team Exercise 1	50
Student Exercise 1	25
Student Exercise 2	25

Grading
250-222 =A=100-90%
221-180= B= 89-80%
179-175= C= 79-70%
174-150=D=69-60 %
149 below=F= 59-0%

SIS 1XX **Introduction to the Security Profession** **Lesson Plan**
Reference Text: IS=Introduction to Security

Week	Topic Areas	Instructional Methods	Student Assignments
1.	**Security Profession** • Course introduction and overview • Historical Development of the security profession	Classroom Presentation Class Discussion	Read **IS** Chapters 2 Visit Websites: ASIS International USA Jobs
2.	**Security Authority & Organizational Roles** • Defining the role of security in organizations • Private security & law enforcement differences	Classroom Presentation Class Discussion	Read **IS**, Chapter 3-4,

3.	**Security Disciplines** • Physical security • Personnel security Information Security • Information Systems Security • Homeland Security • Critical Infrastructure Security	Classroom Presentation Class Discussion	ASIS Pamphlet ASIS website
4.	**Security Specialty Areas** • Bank security • Hospital security • Institution School • Govt/Industrial Security		ASIS Pamphlet ASIS website
5.	**Government Security Careers** • Security Officer-IC Organizations • Federal Law Enforcement • Regional Security Officers • Industrial Security Officers		Read Handouts GS-0080
6.	**Guest Lecturer**- Security Professional Research security careers		
7.	**Private Security Careers** • Corporate security managers • Security Consultants • Private Detective • Security Services • Security Equipment		ASIS Handout Read IS, Chapter 5

8.	**Guest Lecturer**- Security Professional Research security careers	Class Discussion	Individual research Assignments
9.	**Personal and professional integrity** Ethical behavior Background Investigations	Classroom presentation and Discussion Quiz 1	ASIS Code of Conduct
10.	**Individual Exercise 1 Presentations**		
11.	**Security & Employee Training** • Security Procedures • Equipment Operations		Read IS, Chapter 6
12.	**Professional Career Planning**	Classroom discussion	
13.	**Individual Exercise 2**	Classroom discussion Quiz 3 Briefings and Discussion	
14.	**School Holidays**		
15.	**Team Projects** • Presentations • Discussions • Peer critiques Teams present their solutions and decision process		3
16.	**Course Review & Student Learning Assessment** • Quiz 3		

Course Number: SIS 2XX **Credit Hours: 3**

Title: Security Fundamentals

Required Texts:

1. Fisher, Halibozack and Walters, Introduction to Security, *8nd Edition.* Butterworth & Heinemann ,Sebastopol, CA, USA : (2008),
2. Solomon & Chapple, Information Security Illuminated, Jones and Barlett Publishers, Sudbury, MA (2005)
3. I David G. Patterson, CPP, PSP, Physical Protection Systems: Implementing Physical Security Systems, A practical Guide , ASIS International (2004)
4. Supplementary Readings: Reading assignments and reference items provided by instructor.
    a) ASIS International. (2007). Protection of Assets . Alexandria: ASIS International
    b) U.S. Department of Army, Field Manual 3-19.30, Pysical Security , DOA, January 8, 2001

Course Description: This course provides students with a familiarity with the general concepts of security, threat assessment, personnel security, physical security and information security both the government and private sectors. Students will learn the importance of applying proper security protection measures to protect an organizations personnel, physical assets, and sensitive information. Students will learn the basic personnel security screening methods, the general types of security equipment and its protective applications, the ways of protecting both sensitive information and computer systems storing and transmitting such information. The students will also learn the basic methodology for conducting investigations in private and government organizations.

Goals: The goal of this course is to provide the student with a general understanding of security and threat assessment concepts. The student will also learn the basics of personnel, physical and information security as practiced in government and private organizations. The knowledge and skill sets developed in this course form the foundation for the latter security courses that focus on the applications of these principles and protective measures in various threat situations in both the government and private sectors.

Learning Outcomes:

1. Understand general security principles and practices as they apply to the protection of government and private organizations and facilities

2. Understand basic risk management and threat assessment concepts and applications

3. Be familiar with entry control and access control systems

4. Be familiar with perimeter security concepts and equipment applications

5. Be knowledgeable of personnel best security policies and practices

6. Understand the practical and legal constraints on the use of close circuit video and audio surveillance equipment

7. Be familiar with the range of security measures employed to protect sensitive and classified information to include best practices, computer operating system and network security information and communications security

8. Understand digital evidence recovery, collection and the legal requirements for such collection.

9. Appreciate the vital importance of security to the United States social, political, military and economic well being

10. Be familiar with basic investigative approach and legal constraints used to conduct background investigations, civil and criminal investigations and administrative investigations

11. Produce professional (individual and group) quality reports and presentations.

Description of Assessment Activities:

Mid-Term Examination: The examination will assess the student‘s knowledge and understanding of basic security concepts, security organization and management, legal issues, risk management and threat assessment, physical security concepts and equipment, and personnel security measures. The written test will consist of a combination of essay and short answer questions to test their overall knowledge and several scenarios to evaluate the student‘s understanding of the practical application of these concepts and techniques.

Final Exam: The examination will assess the student‘s comprehensive knowledge and understanding of security concepts and principles, risk management and threat assessment, physical security concepts and equipment, and personnel security measures , emergency and contingency planning, workplace violence, information and computer security , transportation security, and terrorism against the United States. The written test will consist of a combination of essay questions and practical scenarios to evaluate the student‘s overall knowledge and their ability to apply the knowledge in real-world scenarios.

Class Activities:

Team Exercise 1 – Construct a fictitious government or business organization based on available public information. This team exercise will require the team to research organizational structures, personnel staffing levels, financial information to create a realistic organization. The instructor will review their organizational structure, staffing, and financial basis and provide comments.

Team Exercise 2 – Organize and staff a proposed security department for the fictitious organization along with developing the supporting department expense budget. The team must determine the most effective reporting level for the senior security manager, the titles and functions of his or her subordinates and their proposed locations within the organization. The instructor will review and evaluate each team‘s proposed security organization and provide feedback.

Team Exercise 3 – Conduct a risk management assessment of a new proposed faculty using information provided by the instructor. The team must apply a risk assessment model to identify all the hazards, determine their likelihood, the vulnerabilities of the faculty and the criticality to the faculty should such an event occur. Brief the class and instructor on their risk assessment and priority resource allocation.

Team Exercise 4 – Identify and select the most effective security equipment to purchase and install in the new facility. The team must identify, select, and cost out all of the equipment that believe to be warranted by the threats identified. They must also develop a capital budget for the new facility. The team must brief the instructor and their classmates of their results with a formal power point presentation**.**

Student Exercise 1 – Draft a workplace policy and procedure for their team's organization. This exercise is designed to allow the individual student to apply concepts and principles learned in a practical manner and to allow students to practice policy and procedure writing skills. The instructor will evaluate and provide feedback to the individual student.

Student Exercise 2 – Draft a basic information security policy to ensure employee awareness and protection of company sensitive or government classified material. This exercise is designed to allow the individual student to apply information security concepts and principles learned in a practical manner and to allow students to practice policy and procedure writing skills the instructor will evaluate and provide feedback to the individual student

Scoring and Grading Matrix

Scoring Area	**Maximum Points**
Team Exercise 1	50
Team Exercise 2	50
Team Exercise 3	50
Team Exercise 4	50
Student Exercise 1	25
Student Exercise 2	25
Final Examination	50

Grading
300-270-222 =A=100-90%
269-240= B= 89-80%
239-210= C= 79-70%
219-180=D=69-60 %
179 below=F= 59-0%

SIS 2XX Security Fundamentals Lesson Plan

Week	Topic Areas	Instructional Methods	Student Assignments
1.	**Security Profession** • Course introduction and overview • Historical Development of the security profession • Career Opportunities & education	Classroom Presentation Class Discussion	Read **IS** Chapters 2,5, 6 Read **FM**, Chapter 1 Visit Websites: ASIS International DNI USA Jobs
2.	**Security Authority & Organizational Roles** • Defining the role of security in organizations • Contract vs. proprietary security • Private security & law enforcement differences	Team Project 1 Individual Exercise 1	Read **IS**, Chapter 3-4,
3.	**Security & the Law** • Sources of law • Civil and criminal law • US court systems • Private security powers		Read **IS** Chapter 7
4.	**Risk Management** • Concepts • General Approaches to Risk Management • Threat Identification • Natural and Manmade	Team Project 2	Read **IS** Chapter 8, Read Handouts
5.	**Threat Assessment** • Threat Assessment Models • Threat Levels • Vulnerability factors • Criticality • Threat Assessment	Class Discussion Practical Threat Assessment Exercise Team Project 2	Team Assignments

	Matrix		
6.	**Security Through Design Concepts & applications** • Approaches to Physical Security • Area and Perimeter Security • Points of Ingress & Egress • Interior Space Protection • Fire & Safety Concerns • Perimeter security devices • Physical Security Equipment	Classroom presentation and discussion	Read **IS** Chapters 9 & 10 Read **FM**, Chapter 2,3, 4 & 5 Read Handouts
7.	**Intrusion detection, access control and surveillance** • Locks & key control • Files, safes, vaults • Alarm systems & sensors • Access control systems • CCTV surveillance • Intrusion Detection Systems • Security Personnel & Patrols	Team Project 3	Read **IS** Chapter 11, Read Handouts Read **FM** Chapters 6,7,8
8.	**Personnel security** • Employment checks • Background investigation • Policies and procedures	Individual Exercise 2	Read **IS** Chapter 13, Read FM Section 7-1 Read Handouts Individual Practical Project
9.	**Mid- Term Review & Examination** • Basic Security Concepts & Applications • Post Examination Review	Classroom discussion	Read Handouts Assignment of Team Projects
10.	**Emergency Operations & Response** • Security Response	Classroom discussion	Read **IS** Chapter s 9 &12 Student Exercise 4-

	• Emergency Evacuation • Bomb Threat • Contingency Planning Crisis management		Draft an emergency evacuation plan
11.	**Workplace Violence & Illegal Drug Use** • Emergency response • Employee Awareness • Drug Abuse Policies • Workplace Drug Testing • Drug Free Workplace		Read **IS ,**Chapter 15 Problem Solving Exercise 2 Individual Practical Project
12.	**Information & Computer Security** • Information security programs & procedures • Government classification systems • National Industrial Security Program • Computer & Network security basics •		Read IS ,Chapter 18 Security Problem Solving Exercise 3
13.	• **Team Projects** • Team Project Meetings • Team Project Presentations • Peer Review Sessions	Team Project 4	
14.	**Security & Employee Training** • Security Procedures • Equipment Operations • Information Protection Issues • High Rise Protection Issues		Read IS, Chapter
15.	**Terrorism Against the U.S.** • US Intelligence & Law Enforcement Agencies • Government Employees & Facilities • Commercial		Read **IS** Chapters 1, 17 , 19

	Organizations		
16.	**Course Review & Student Learning Assessment** a) Comprehensive Course Review b) Written Final Examination		

Course Number: SIS 295 **Credit Hours: 3**

Title: Introduction to Intelligence Writing

Required Texts:

1. Brooks Jackson and Kathleen Hall Jamieson, un.Spun: Finding Facts in a World of Disinformation, New York: Random House, 2007.

2. James S. Major, Writing Classified and Unclassified Papers for National Security, Lanham MD: The Scarecrow Press, Inc., 2009.

3. William Strunk, Jr. and E.B. White, The Elements of Style, Fourth Edition, New York: Longman, 2000.

4. *The New York Times.* The student is encouraged to take at least a five-day student subscription to *The New York Times.* A full seven-day subscription is recommended as the Saturday paper always has a section on ideas and philosophy, while the Sunday paper has excellent resources including the "Magazine," the "Week in Review," and the "Book Review" section.

Alternatively, the student can take a student subscription to either *The Wall Street Journal* or *The Financial Times* of London or can access the *Christian Science Monitor* which is now only on-line. In addition, the student should stay in touch with internet news sources such as www.bbc.co.uk, www.cnn.com, www.globalsecurity.org, and www.stratfor.com. Check the library for subscriptions available for additional resources.

Course Description: The purpose of this course is to teach the basic skills of intelligence writing. The most essential principle of intelligence writing is to communicate to the reader exactly the message the analyst wants to communicate. Clarity, precision, accuracy and brevity are key elements of intelligence writing; however, it is also crucial that analysts understand the overall structure of the intelligence brief. An intelligence brief communicates, as quickly as possible, the circumstances of a development and its meaning or implication for the reader. The audience for an intelligence brief is usually a senior official who has no time to peruse long and

complex reports. They need to absorb the information and understand its implications in the shortest time possible and determine whether action must be taken. Within this course, two other elements will be covered intensively as part of the intelligence writing process: 1) a capacity to accurately evaluate information and 2) a capacity that leads to making analytical judgments about the significance of a development.

Goals: As an introduction to the science and art of intelligence writing, SIS 295, Section 1 is essential for the student pursuing a B.S. Degree in Global Security and Intelligence Studies (GSIS) and serves as a prerequisite to SIS 328, *Intelligence Analysis, Writing and Briefing.* The capacity to communicate in writing is a fundamental skill without which an individual will be unable to succeed in most areas of intelligence work. For the analyst, potentially seeking a career in the Intelligence Community, Homeland Security, the corporate and business world, or the military, it is essential. The capacity for practical as well as intellectual work is a key feature of higher education at Embry Riddle Aeronautical University. As numbers of our GSIS graduates have shown, the capability to sit down and produce an intelligence brief, virtually upon entering on duty, has surprised and delighted managers and enabled these graduates to start their careers on a high note. An added advantage is that the student‘s writing in other courses and fields of study will markedly improve. The student will be given the opportunity to develop critical thinking and reading skills, the principles of intelligence writing, evaluating sources and analytical frameworks

Learning Objectives:

1. Discuss, in depth, an assigned account including current and changing situations; implications of geo-strategic position, if applicable; impact of major issues such as political, sociological, or historical; and major trends underway.

2. Evaluate new data or information about the assigned account avoiding opinion and substantiating information such as sources. Identify understanding of ideological or religious forces as social movements accessible to objective analysis.

3. Identify the principles of intelligence writing and intelligence briefing.

4. Write talking points for presentation to a senior official.

5. Demonstrate analysis of complex developments by providing clear written language that will allow the consumer to understand and act upon the information.

6. Identify ―spin.”

Student Assessment:

Grading Scheme

Category (each)	Points	Comments
Account Profile	100	Profiles will be evaluated and either accepted or a resubmit will be requested.
Quiz	100	There will be four quizzes based on information from the textbooks; each can earn 1-25 points.
Class Participation	100	To be successful in this course, the student needs to be prepared for each class session as well as be willing and interested in participating.
Intelligence Briefs	200	Upon submission and approval of your account profile, begin writing a weekly intelligence brief. As a key part of the course, some of these briefs will be edited in class; some after class. Requires submission of no fewer than 10 intelligence briefs, each can earn 1-20 points.
Mid-term exam	100	Points = 100
Talking Points	100	As a rapid reaction form of intelligence writing, the student will produce, on a tight deadline, talking points for presentation to a senior official. We will practice this in class then you will produce talking points for an intelligence briefing.
Intelligence Article	100	Write an intelligence article of two to three pages, double-spaced – an expanded form of the intelligence brief format
Production Folder	100	To be submitted at the end of the course and will include all work and supporting documentation. Points = 100
Final exam	100	Points = 100
Total Possible Points		**1000**

Final Grade: Your final grade will be based on your final number of points earned out of a possible 1,000.

A	90% or better	900-1000 points
B	80%-89%	800-899 points
C	70%-79%	700-799 points
D	60%-69%	600-699 points

Class Activities:

Account Requirements: The following keywords are *suggestions* to consider when ~~re~~ading in" to your account. It is important not only to gather factual data but to also understand the intertwining of different strata as they relate to your account. This is the kind of information that will allow you to become knowledgeable about your account and prepared to address changes and the implications of those changes.

Political system	Climate
Economic (assets, debt)	Military (order of battle)
Geography	Population
Society	Weather
Environmental	International Agreements
Religion	Ethnicity of population
Languages	Communications

Production Folder Requirements (end-of-course submission) your production folder will be turned in at the end of the course and will contain, at a minimum, the following:

- Your Account profile
- All original intelligence briefs with edits and your rewritten briefs
- Your talking points
- Your final intelligence article
- All supporting materials for your account.

Class Policies: Vary with the institution and instructor preferences

SIS 295 Introduction to Intelligence Writing Lesson Plan

Class Meetings	Assignments
Week 1 • Six fundamental principles of writing • How word choice impacts on message	General Overview of Course and Discussion of Requirements

Class Meetings	Assignments
• Four major areas to improve writing (spelling, word usage, punctuation, and subject-verb agreement) • Working titles for intelligence writing • Purpose of headings and sub-headings • Importance of document layout • Using graphic material within writing	Introductions **Reading Assignments:** Writing Classified and Unclassified Papers for National Security James S. Major **Accounts:** You will find out this week what your account will be for the remainder of the semester and we will review specific requirements for the Account Profile. You will then begin to ~~r~~ead-in" on your account.
Week 2 • Difference between information and intelligence • Differences between academic writing and intelligence writing • Four step framework for analysis • Thesis statement • Methods to coax information from memory • Supporting the thesis statement through induction or deduction	**Reading Assignments:** Writing Classified and Unclassified Papers for National Security James S. Major Chapter 3 Chapter 4
Week 3 • Intelligence brief format • Dangers of Seville Marketing's claims • Concept of ~~s~~pin" • Conspiracy theories.	**Reading Assignments:** un.Spun: Finding facts in a world of disinformation Brooks Jackson & Kathleen Hall Jamieson Chapter 1 **Account Profile:**
Week 4 • ~~F~~UD" • A dangling comparative • Superlative. • ~~G~~littering Generalities".	**Reading Assignments:** un.Spun: Finding facts in a world of disinformation Brooks Jackson & Kathleen Hall Jamieson Chapter 2 **Intelligence Brief #1:** **Quiz #1:**

Class Meetings	Assignments

Week 5
 	
• Common tricks of the deception trade
  o Misnomer
  o Frame it and claim it
  o Weasel words
  o Eye candy
  o The ―average" bear
  o The baseline bluff
  o The literally true falsehood
  o The implied falsehood
	Reading Assignments: un.Spun: Finding facts in a world of disinformation
	
	Brooks Jackson & Kathleen Hall Jamieson
	
	Chapter 3
	
	Intelligence Brief #2:

Week 6 • ―Barking moonbat" • Cognitive dissonance • The psychology of deception • Four psychological traps that lead to ignoring facts or believing bad information	**Reading Assignments:** un.Spun: Finding facts in a world of disinformation Brooks Jackson & Kathleen Hall Jamieson Chapter 4 **Intelligence Brief #3:**
Week 7 • Price-equals-quality fallacy • ―Facts" about food allergies that can kill you • The military duty to lie • ―All warfare is based on deception" Sun Tzu • Availability heuristic	**Reading Assignments:** un.Spun: Finding facts in a world of disinformation Brooks Jackson & Kathleen Hall Jamieson Chapter 5 **Intelligence Brief #4:** **Quiz #2:**
Week 8 • **Mid-Term Exam:**	**Intelligence Brief #5:** **Intelligence Brief #6:** (Due TBD)
Week 9 • Distinguish between evidence and random anecdotes. • Define anecdotal evidence. • Describe interpretation of the parts of an elephant by six blind men. • Discuss ―data in the service of ideology."	**Reading Assignments:** un.Spun: Finding facts in a world of disinformation Brooks Jackson & Kathleen Hall Jamieson Chapter 6

Class Meetings	Assignments
• Identify nine guides to testing evidence • Discuss six questions to ask about a factual claim. • Define *post hoc, ergo propter hoc*	

Week 10
 	
• The Internet solution
• Investigate the following:
  o Snopes.com
  o Factcheck.org
  o Alexia.com
  o Technorati.com
  o lii.org
  o Drudge report
• Importance of verifying sources of information
• Ten ―mostly" reliable and unbiased Internet sites
• Questions that should be asked when practicing due diligence
	Reading Assignments: un.Spun: Finding facts in a world of disinformation
	
	Brooks Jackson & Kathleen Hall Jamieson
	
	Chapter 7
	
	Intelligence Brief #7:

Week 11 • Finding facts in a world of disinformation • Nine rules for verifying facts • ―Consensus isn't proof" • The importance of primary sources • Numerical and statistical tricks to prove information is factual • Methods of weighing evidence to cross-check facts	**Reading Assignments:** un.Spun: Finding facts in a world of disinformation Brooks Jackson & Kathleen Hall Jamieson Chapter 8 **Intelligence Brief #8:**
Week 12 • Using who, what, where, when, why, and how in building talking points • Briefing techniques • Purpose of briefing a senior official	**Intelligence Brief #9:** **Quiz #3:**
Week 13 • Skills in oral presentation • Short update of development in account deliverable to peers	**Intelligence Brief #10**

Class Meetings	Assignments
• Short update of development in account deliverable to senior officials	
Week 14 • Requirements for Intelligence Article • Skills in oral presentation • Short update of development in account deliverable to peers • Short update of development in account deliverable to senior officials	**Presentations:** Talking Points **Quiz #4:** **Intelligence Article** (
Week 15 • Skills in oral presentation • Short update of development in account deliverable to peers • Short update of development in account deliverable to senior officials **Week 16 Final Examination**	**Presentations:** Talking Points

Course Number: SIS 325 **Credit Hours: 3**

Title: History of Terrorism

Required Texts

1. Randall D. Law, Terrorism: A History, Cambridge, UK: Polity Press, represented in US by Wiley, 2009.
2. Jonathan R. White, Terrorism and Homeland Security, Belmont, CA: Thomson-Wadsworth, 7th edition, 2011.

Course Description: SIS 325 examines the historic roots of terrorism including its development and practice worldwide. The course will examine terrorist organizations and events through themes and ideologies that will introduce the student to the history of terrorism, from the ancient world to the present day. It will evaluate the causes of terrorism, the capabilities and limitations of terrorist groups, the requisites of effective counter terrorism responses, and the future prospects of terrorism. Constitutional and legal implications of counterterrorist strategies will also be discussed. SIS 325 will examine the organization, objectives, and methodologies of key

international and domestic terrorist groups operating in the 21st century, particularly those showing ideological hardening, religious revivalism, and ethnic militancy.
(Prerequisites: SS 110)

Goals: This course is required for students in the Global Security and Intelligence Studies (GSIS) program. It should also be of interest to students interested in military careers, global business, engineering, and aeronautical science.

The course will examine different types of terrorism, the technologies used by terrorist groups, and the impact of terrorism and terrorist groups upon the foreign policies of nations. Teaching strategies may include lectures, demonstrations, practical exercises, case studies, role-playing, and group collaboration. In addition to text readings, supplemental readings and research will support exercises and class discussions to apply content.

Learning Objectives: This course is designed to introduce upper level students to the origins and impacts of various terrorist movements within a global context. As such, at the end of the course the student will be able to:

1. Develop chronological knowledge of terrorist groups within an historical context using an ideological or thematic approach.

2. Identify the origins and operations of various terrorist organizations world-wide.
3. Discuss the underlying reasons for the development of terrorist organizations and national governmental reactions to their activities.

4. Identify governmental programs designed to thwart the activities of terrorist organizations.

Grading and Class Requirements:

Category (each)	Points	Comments
Activities	10	Each activity can earn 1-10 points Points = 200
Papers	25	Each paper can earn 1-25 points Points = 250
Individual Presentation	10	One individual presentation is required and earns 1-25 points. Other presentations are on voluntary basis, as time permits, and can earn between 1-10 points. Points = 25
Mid-term exam	100	Points = 100
Final exam	100	Points = 100
Group Presentation (Major class project)	50	This activity will include 25 points for individual participation; 25 points for group participation. Document all activity. Presentation minimum 20 minutes; maximum 30 minutes

		Points = 50
Class Participation	45	To be successful in this course, the student needs to be prepared for each class session as well as be willing and interested in participating. Points = 50
Total Possible Points		**775**

Student Portfolio Requirements

- Activity submissions are to be a minimum of 250 words; maximum of 350 words. In developing your commentary, think, analyze, and condense. Submissions are electronic. Cite sources at the bottom of page rather than on a separate page. Be sure to keep a copy for your records. In the header, use the following example as format:
    - Smith, John R
    - SIS 325 – Fall 2011
    - Date

- Paper submissions are to be typed, double spaced and preferably submitted electronically. Papers to be a minimum of 3 pages (not including references); maximum of 5 pages. Avoid Wikipedia as a primary source – you may use it as a secondary source. Be aware of sites visited when researching; remember, if you can access their web site, they know who you are by your IP. On a separate page, cite references accessed (even if not used) and if using direct quotes in paper, identify source by placing author and date in parentheses following the quotation (ex: Smith, 2011). Be sure to keep a copy for your records. In the header, use the following example as format:

    - Smith, John R
    - SIS 325 – Fall 2011
    - Date

- One required individual oral presentation. Prepare for no less than 5 minutes and no more than 10 minutes. You will be stopped if time exceeds 10 minutes and points will be deducted. Visuals and graphics are encouraged; PowerPoint may be used to supplement presentation, if applicable. Do not read PowerPoint slides if used; this will reduce points. An outline of the presentation is to be prepared for the instructor.

- Portfolio equates to a major portion of your grade for this class. Do not fall behind and lose points for late submission. Weekly options will be presented at the beginning of each week with submissions due NLT first day of class of the following week. Submissions may be made earlier if completed.

Final Grade: Your final grade will be based on your final number of points earned in the class.

A	90% or better	697-775 points
B	80%-89%	620-696 points
C	70%-79%	542-619 points
D	60%-69%	465-541 points

Class Policies: vary with institution‘s and instructor‘s preference

SIS 295 Introduction to Intelligence Writing Lesson Plan

Week 1 Social contexts of terrorism Typologies of terrorism The war on terrorism Networks and law enforcement Impact of asymmetrical warfare •Practical criminology •Elements of netwar •Terrorism as a religious process •Eight primary cultural paradigms •Profiling debate •Processes of radicalization		General Overview of Course and Discussion of Requirements Introductions Reading Assignments: Terrorism & Homeland Security, seventh edition Jonathan R. White Chapter 1 Chapter 2 Weekly Portfolio #1: Distribute portfolio options for activities (select 2) and short paper (select 1).
Week 2 Rural, urban and insurgent models of terrorism •Evolution of terrorist organizational structures •Terrorist financing •Piracy •Legal and illegal sources of income for terrorist groups •The Hawala system •Narcoterrorism •Role of media •Relationship between terrorism and television •Issues surrounding objective reporting		Reading Assignments: Terrorism & Homeland Security, seventh edition Jonathan R. White Chapter 3 Chapter 4 Weekly Portfolio#2: Distribute portfolio options for activities (select 2) and short paper (select 1).

Week 3 Gender and group ideology •Historical importance of female terrorists •Tactics of modern terrorism •Force multipliers •Threats posed by cyberterrorism •CBRN •Transnational economic targeting •Theories and logic of suicide terrorism •Terror and tyrrannicide in the ancient world •Assyrians, Greeks, Romans, Indians, Hebrews •Case Study of the Sicarii •Church, State, and violence in Medieval Europe •Medieval Islamic world •The assassins •	Quiz #1 Discussion of Portfolio Activities	Reading Assignments: Terrorism & Homeland Security, seventh edition Jonathan R. White Chapter 5 Terrorism: A History Randall D. Law Chapter 1 Chapter 2 Weekly Portfolio #3: Distribute portfolio options for activities (select 2) and short paper (select 1).
Week 4 The Renaissance and Tyrannicide •State sponsored assassination in the Renaissance •Machiavelli •The Reformation and Tyrannicide •English Tyrannicide •The English Civil War •Tyrannicide in Medieval and Early Modern Europe •The Anabaptists of Munster and Secret Societies •L'Ancien Regime and the French Revolution •The Reign of Terror •The Restoration and Conservatism •Revolutionary Secret Societies •Babeuf and Buonarroti •The Carbonari •The Luddites		Reading Assignments: Terrorism: A History Randall D. Law Chapter 3 Chapter 4 Terrorism & Homeland Security, Seventh Edition Jonathan R. White Chapter 6 (due 07 Oct) Weekly Portfolio #4: Distribute portfolio options for activities (select 3) and short paper (select 1). Portfolio Submissions

•Heinzen and Conspiratorial Terrorism		
Week 5 • Return and discuss mid-term exam. • 10-minute Student Class Presentations	• Assign and discuss requirements for final presentation on specific terrorist group.	• Law – pp. 233-245 The Irish Republican Army • White – pp. 197-203 The Modern IRA
Week 6 Sri Lanka Tamil Tigers Basque Nation and Liberty (ETA) 20th Century Basque Nationalism and ETA Palestinians, Arafat, and the PLO	• 10-minute Student Class Presentations	• Law – pp. 217-233 • Law – pp. 245-249 • White – p. 210-215 • Law – pp. 249-251 • White – pp. 204-210 • Law – pp. 217-233
Week 7 Terrorism in Israel and Palestine	Class Discussions	• White – pp. 290-325 • White – pp. 290-325
Week 8 Tupamaros, Shining Path, Weathermen, Symbionese Liberation Army FARC Aum Shinrikyo	Class Discussions	• Law – pp. 254-271 • White – pp. 338-354 • White – pp. 361-362 • White – pp. 370-371 • White – pp. 427-466 Domestic Terrorism • White – pp. 471-503 Homeland Security
Week 9 White Supremacy and the KKK	Class Discussions	• Law – pp. 126-139
Week 10 Rise of Jihadist Terrorism and Islam Background Jihadist, Bin Laden, Zawahiri, al-Qaeda	Class Discussions	• Law – pp. 281-314 • White – pp. 378-389
Week 11 Jihadist, Bin Laden, Zawahiri, al-Qaeda	Class Discussions	• White – pp. 399-401

Role of Women in Terrorism		
Week 12 • Group Presentations on Individual Terrorist Organizations	Group Presentations	
Week 13 • Group Presentations on Individual Terrorist Organizations	Group Presentations	
Week 14 • Group Presentations on Individual Terrorist Organizations	Group Presentations	
Week 15 Review for Exam	Review of course information	
Week 16 Final Examination		

Course Number: SIS 100 **Credit Hours: 3**

Title: Introduction to Global security and Intelligence

Required Texts:

1. Linda Elder and Richard Paul, The Foundations of Analytic Thinking (Dillon Beach, CA: The Foundation for Critical Thinking, 2003)
2. Robert M. Jackson, ed., Global Issues, 11/12 (27th ed., Guilford, CN: McGraw Hill/Dushkin, 2011).
3. Robert D. Kaplan, Warrior Politics: Why Leadership Demands a Pagan Ethos (New York: Random House, 2002).
4. Rudyard Kipling, Kim (Oxford: World Classics, 2008).
5. The New York Times. The student is encouraged to take at least a five-day student subscription to The New York Times or another national paper. For those taking The New York Times, a full seven day subscription is recommended, as the Saturday paper always has

a section on ideas and philosophy; while the Sunday paper has the –Magazine," –Week in Review," and –Book Review" –all excellent resources. Alternatively, the student can take a student subscription to either The Wall Street Journal, Christian Science Monitor (now available only on-line) or The Financial Times of London. In addition, the student should stay in touch with internet news sources, such as www.bbc.co.uk, www.cnn.com; www.globalsecurity.org; and STATFOR, to which we have a subscription that is available through the Library.

Course Description: This course will cover and emphasize the elements of critical thinking, as well as introduce the student to key ideas propounded by –great thinkers," such as Thucydides, Sun Tzu, and Churchill. The course also will examine critically the major cultural, economic, environmental, international and other –civilization" issues of the contemporary epoch. The course will pursue an understanding of the underlying –structure" of the post-modern epoch—of its economic requisites and demographics, of the ideas that shape it, of the uses of power in the international system, of the choices that lie before us, and of the broader policy implications of those choices. The course will be shaped by three main elements: (1) an examination of the methods for critically analyzing and understanding contemporary issues; (2) a familiarization with the relevant terms and concepts; and (3) an overview of the main themes in Global Security and Intelligence Studies (GSIS), as well as several in-depth examples of importance to GSIS students.

Goals: SIS 100 is required for all students pursuing the B.S. degree in the GSIS Program. The goal of the course is to familiarize first year students with those overlapping –areas of knowledge" vital to understanding the increasingly complex and integrated—or global—world of today and the future.

Learning Outcomes:

1. Become familiar with the content of the course, the issues discussed and the ideas raised. This means to be able to describe these issues and ideas, the pros and cons of each, the knowledge areas they represent, the interconnectedness of these, and of how various issue groups states its case.
2. Demonstrate a capability to think critically and analytically. Look for supporting data when making assertions and work to structure a presentation around reasoned arguments.
3. Learn to speak and write informatively and clearly.
4. Demonstrate and understanding of how the issues and ideas discussed in the course relate to the curriculum of your major, the particular requirements of the career you will undertake the requisites of good citizenship, and the pursuit of truth.
5. Be able to make up your own mind about where you will stand on these issues. This is a purely personal activity—the course does not take a particular position or require you to do so, but it does ask you to be clear, analytical, reasoned, and able to marshal agreed data to support your views. Passion about ideas is fine; but passion without substance will not take us very far.

Description of Assessment Activities:

Final Grade: The final grade you **earn** will be based on your final number out of a possible 700—or more if quizzes are given. Anyone achieving 90% or more of the total possible will earn an A; 80-89% a B; 70-79% a C; 60-69% a D. So, for a 700 point total, the grades will fall out as follows:

A: 630 to 700 total points

B: 560 to 629 total points

C: 490 to 559 total points

D: 420 to 489 total points

Class Participation. Participation in class discussions, reports, and projects is an important part of the class. Each class with begin with a review of international developments over the past 24 hours. Learning to summarize a news story or topical article and present ideas and analysis is a lifelong skill. At a minimum, you, the student, will tell the class about an interesting development in international relations, national policy, science or nature, the environment, a newly published and widely acclaimed book, an event in the business world, etc. You may report as often as time permits, with priority first given to those who are speaking up for the first time. **(100 possible points).**

Book Review. A review of the novel Kim is assigned of up to 5/6 pages, double-spaced. Your review should give an overview of the novel. What is the story about? Are there several levels of meaning in the novel? What is the author‘s attitude to the government of the British Raj? How does the author see human nature? What does the novel tell you about the requirements of being an intelligence officer, a spy? (100 possible points)

Midterm Examination. The examination will assess the student‘s knowledge and understanding of the course material and understanding of the global security and intelligence study area. **(100 possible points).**

Team Presentation. You will be assigned to a team that will prepare a presentation during the second half of the semester on one of the topics in Global Issues . This exercise will challenge you to get inside an issue, understand the assumptions the author has, understand the quality of the data, analyze the policy implications, and come up with some solutions. It will expand your knowledge and your capacity to deal with knowledge. It will give you a chance to verbalize your arguments and views and to make a cogent presentation. It also will help to mix up the class and enable you to get to know some of the others in these unique degree programs. This is a significant part of your grade. Each student in the team will participate in the presentation. Your

grade will be composed of a team grade (100 points) and an individual grade (100 points) for **200 possible points.**

Final Exam: This comprehensive examination will assess the student‘s knowledge and understanding of the course material and understanding of the global security and intelligence study area (**200 possible points.**

SIS 100 Introduction to Global Security and Intelligence Lesson Plan

Week	Topic Areas	Instructional Methods	Student Assignments
1.	Introduction to the Course Realism, Idealism and the _In Between‘ Thinking Critically	Classroom Presentation Class Discussion	Kaplan, Ch 1, 2 Elder and Paul
2.	Livy, Sun Tzu, Thucydides Machiavelli		Kaplan, Ch 3, 4, 5
3.	GSIS Program elements		Kipling, Kim
4.	**The Master Student**	Student and Instructor discussions	Kipling, Kim Analytical Thinking Elder and Paul
5.	Hobbes, Malthus, Kant, Achilles, China and Tiberius	Class Discussion	Kaplan, Ch 5-11 Kim
6.	Discussion: Kipling‘s	Classroom presentation and discussion	Kim
7.	14 Global Issues	Classroom presentation and discussion Mid-Term Exam	Jackson, Units 1, 2
8.	Team One: Global Envir. 1 Team Two: Global Envir. 2 Articles 12, 13, 14	Team presentations	Jackson, Unit 3

9.	Team Three: Political Economy Articles 18, 19, 20, 21 Team Four: Political Economy 2 Articles 22, 23, 24, 25	Team presentations	Jackson, Unit 4
10.	Team Seven: Conflict 1Articles 32, 33, 34, 35 Team Eight: Conflict 2 Articles 36, 37, 38	Team Presentations	Jackson, Unit 4
11.	Team Seven: Conflict 1Articles 32, 33, 34, 35 Team Eight: Conflict 2 Articles 36, 37, 38	Team Presentations	Jackson, Unit 5
12.	Team Nine: Cooperation Team Ten: Values and Visions	Team Presentations	Jackson, Unit 6 Jackson, Unit 7
13.	Open	To Be Determined	
14.	School Holiday Break		
15.	Course Review		
16.	Student Learning Assessment Written Final Examination		

Course Number: SIS 315 **Credit Hours: 3**

Title: Global Intelligence Studies I

Required Texts:

1. Mark M. Lowenthal, Intelligence: From Secrets to Policy (Fourth Edition, Washington, D.C.: Congressional Quarterly Press, 2009).

2. Colonel John Hughes-Wilson, Military Intelligence Blunders (Revised ed., New York: Carroll and Graf Publishers, 2004).
3. Robert Baer, See No Evil: The True Story of a Ground Soldier in the CIA's War on Terrorism (New York: Three Rivers Press, 2002).

Also Recommended:

a. The 9/11 Commission Report: Final Report of the National Commission on Terrorist Attacks Upon the United States (Authorized Edition, New York: WW Norton, 2004)
b. Christopher Andrew and Vasili Mitrokhin, The Sword and the Shield: The Mitrokhin Archive and the Secret History of the KGB (New York: Basic Books, 1995).
c. Anthony Cave Brown, Bodyguard of Lies (New York: Harper and Row, 1975).
d. Richard Helms, A Look Over My Shoulder: A Life in the Central Intelligence Agency (New York: Ballentine, 2003).
e. Floyd L. Paseman, A Spy's Journey: A CIA Memoir (St. Paul: Zenith Press, 2004).
f. Jeffrey T. Richelson, A Century of Spies: Intelligence in the Twentieth Century (New York: Oxford University Press, 1995).

Course Description: SIS 315 will examine the uses of strategic intelligence by world leaders in shaping policy and the effects of strategic intelligence on world events. The course will focus on primarily—but not exclusively—on the historical, modern, and contemporary role of intelligence in United States foreign relations and in those of its allies and opponents. Issues to be covered include theoretical models of strategic intelligence; intelligence collection, evaluation, analysis, production, and dissemination; intelligence oversight; covert and clandestine operations; intelligence bureaucracies; ethical and moral issues in intelligence; counterintelligence. Case studies will be used to elucidate these aspects. Case studies include Pearl Harbor, Operation Barbarossa, the Bay of Pigs, the Cuban Missile Crisis, the Iran Hostage Rescue Mission, and September 11, 2001. The course addresses strategic intelligence in the business, political, military, scientific, and technological domains. It is a lecture and discussion course.

Goals: The course is designed to introduce the student to the institutional structure of the Intelligence Community in the United States, to the statutory authority that underpins the various elements of the community, and the oversight process by Congress. The student also will study the elements and dilemmas in each stage of the intelligence process, the uses of intelligence by the President and his advisers, and the role and effectiveness of covert action. Historical lessons of intelligence successes and failures will be used to elucidate the role and challenges of intelligence in the twenty-first century. Each student will be expected to read the texts assigned, which provide an overall study of the Intelligence Community, case studies of intelligence failures, and one operative's view of the decline of US intelligence operational (clandestine) capabilities prior to September 11, 2001. Each student will make a comparative study of the

intelligence lessons of Pearl Harbor and September 11, 2001 and propose solutions to improve the critical capabilities of the Intelligence Community.

Learning Outcomes: The course is designed to introduce you, the upper level student, to the role and requisites of intelligence in the contemporary world and to demonstrate an understanding of the historical, analytical, and operational parameters of intelligence. The events of 9/11/01 markedly increase the importance of this course for an understanding of threats and complexities of the international system at the outset of the twenty-first century.

1. The student will acquire knowledge of the history of US intelligence since 1941 and be able to explain the requisites of strategic intelligence as evident in case studies of Pearl Harbor, D-Day, Barbarossa, Singapore, and the Cuban Missile Crisis. The student should be able to critically analyze the uses, failures and successes of strategic intelligence in the Cold War, the Gulf War, the events of 9/11, and the war in Iraq. From the case studies, the student will gain an understanding of how our allies and opponents have used strategic intelligence. These include the British, Germans, Soviets, North Vietnamese, Egyptians, Israelis, and the Americans.

2. The student will be able to describe the institutional structure of the Intelligence Community as it has developed in the aftermath of World War Two. The student should be able to explain the significance of the National Security Act (1947) as well as subsequent legislation, regulations and Presidential Findings pertaining to the Intelligence Community.

3. The student will be able to describe and discuss the model of the intelligence process, as well as the variety and capabilities of human and technical collection systems, the interaction between collection systems, and the questions of collection priorities. The student should be able to critically evaluate the problems of deception and counter-intelligence in war and peace, and describe measures to discover and neutralize deception and hostile penetration.

4. The student will be able to recognize critical problems in intelligence, such as _mirror imaging,' _clientitis,' cultural blind spots, _stovepipes,' the separation of intelligence and policy, pressures to politicize intelligence assessments, and bomb damage assessment. The latter case is an example of how intelligence relates to different institutional interests within the community. The student should be able to understand the nature of institutional tensions and the requirements of community wide coordination, particularly in view of the global threat to terrorism.

5. The student should be able to critically analyze current intelligence issues, particularly the reasons for the catastrophic intelligence failure of 9/11, evaluate the solutions

already in place, and propose further solutions. As part of this, the student will have an appreciation of the requisites of covert action, the decline during the 1990s of the community's operational capabilities, and the steps that must be taken to bring US human intelligence collection capabilities and assets to the point where these can meet the unprecedented intelligence challenges facing the United States in the Twenty-first Century.

6. Learn the material in the course and demonstrate knowledge of the history surrounding the major intelligence issues at least since 1939.

7. Follow current international and domestic developments relevant to intelligence issues in media (The New York Times, Wall Street Journal, BBC, NPR, and others) and pursue a more detailed knowledge of the issues behind the news by reading relevant articles in op ed pages, journals of opinion, and academic studies. This includes the whole range of debate in the aftermath of 9/11.

8. Bring to discussions of these issues a capacity for critical thinking and analysis and a capacity to use reasoned arguments when discussing these issues either orally or in writing.

9. Show a capacity to write on breaking international events in an ~~"in~~telligence writing style" that is simple, pointed, easily expresses complex issues, and is quickly absorbed by policy makers.

Description of Assessment Activities:

Final Grade: Your final grade will be based on the total number of points **you earn** out of a possible 700 points. Anyone achieving 90% or more of the total possible will receive an A; 80-89% a B; 70-79% a C; 60-69% a D. Grades are earned, not given.

In Short, then,

A 630 to 700 points

B 560 to 629

C 490 to 559

D 420 to 489

News Briefings and Class Participation You are encouraged to participate in class discussions and reports/stories/op ed opinions in the media about the topics covered in this course.

Following The New York Times will help here. You will have an opportunity at the beginning of each class to raise or report on an intelligence issue being covered in the media. You should raise an issue a minimum of at least once during the semester. Class participation will account for 100 possible points of your final grade.

Book Review Review Baer's See No Evil. What are Baer's main criticisms of the CIA's Directorate of Operations? What would you propose to fix the problem? (100 possible points.)

Midterm Examination The examination will assess the student's knowledge and understanding of the course material. **(100 possible points).**

Course Paper: Write a 10 to 12 page paper on one of the following topics. Be sure to add a bibliography and footnote the sources you use or quote in the paper. This includes paraphrasing and direct quotes from other writers and sources. Do not fail to do this, otherwise you would be plagiarizing other people's work, an offense that would bring you under the university's procedures for academic dishonesty. Papers that go beyond reportage or description and include an analytical section will have a better chance of earning a higher grade. (200 possible points)

A. The Japanese attack on Pearl Harbor and the Al-Qa'ida attack on New York and Washington rank as the two most costly intelligence failures in US history.
B. Twice during the Kennedy Administration the United States faced crises over Cuba, one of which, the Cuban Missile Crisis, brought the US and USSR perilously close to nuclear war. In both crises, intelligence played key roles—indeed, the first crisis, the Bay of Pigs, was a covert operation.
C. Intelligence and Policy Making: The relationship between the intelligence community and the policy maker is a complex one. Presidents often have treated intelligence quite differently.
D. Technical Intelligence and Human Intelligence: These two collection domains have always competed within the intelligence community. The US has excelled at the former, but done less well at the latter. Indeed, some critics of the community say the downgrading of US clandestine capabilities made it much more difficult to pick up the plotting of the attacks on 9/11. The truth is probably more complex than this, but the topic is worth a good look.
E. Covert Action and Blowback: Some covert actions, particularly those that fail to become public, have long lasting negative consequences and often turned substantial sections of the public against clandestine operations
F. Intelligence and Reform: Periodically, the United States Government has undertaken commissions, studies, and reports about how to reform the Intelligence Community.
G. Intelligence and War: How has intelligence been used in our wars? For example, compare and contrast how General George Washington used intelligence in our war of independence with how it was used during the world wars, or in our current wars in Iraq and Afghanistan.

Final Exam: This comprehensive examination will assess the student's knowledge and understanding of the course material.(**200 possible points.**

SIS 315 Global Intelligence Studies II Lesson Plan

Week	Topic Areas	Instructional Methods	Student Assignments
1.	Strategic Intelligence: definition and purposes Strategic Deception: Case Study: D-Day, Strategic Failure: Barbarossa	Classroom Presentation Class Discussion	Lowenthal, Ch 1 Wilson, Ch 2 Wilson, Ch 3
2.	The Evolution of the US Intelligence Community Case Study: Pearl Harbor		Lowenthal, Ch 2, 3 Wilson, Ch 4
3.	Modeling the Intelligence Process Case Study: Dieppe		Lowenthal, Ch 4; Wilson, Ch 1 Wilson, Ch 6
4.	Intelligence Collection. Case Study: Singapore Case Study: Cuban Missile Crisis	Student and Instructor discussions	Lowenthal, Ch 5 Wilson, Ch 5 Col. Penkovsky (Instructor)
5.	Intelligence Analysis Case Study: Tet Offensive Case Study: Yom Kippur	Class Discussion	Lowenthal, Ch 6 Wilson, Ch 7 Wilson, Ch 8
6.	Case Studies: Kim Philby, Aldrich Ames, Robert Hansson (Instructor) Counterintelligence	Classroom presentation and discussion	Lowenthal, Ch 7
7.	Covert Operations Case Studies: Bay of Pigs, Entebbe, Afghanistan (Instructor)	Classroom presentation and discussion Mid-Term Exam	Lowenthal, Chapter 8
8.	The Policy Maker and Intelligence Case Study: The Falklands Case Study: The First Gulf War	Class Discussion	Lowenthal, Ch 9 Wilson, Ch 9 Wilson, Ch 10
9.	Oversight and Accountability Ethical and Moral Issues in Intelligence	Class Discussion	Lowenthal, Ch 10; . Lowenthal, Ch 13

10.	Intelligence Agendas: Old and New	Class Discussion	Lowenthal, Ch 11, 12 Wilson, Ch 11; The 9/11 Commission Report
11.	Foreign Intelligence Services	Class Discussion	Lowenthal, Ch 15
12.	Intelligence Reform	Class Discussion	
13.	Case Study: 9/11: Why did it happen; how did it happen; what are the strategic implications for the United States; what are the implications for the Us Intelligence Community?	Class Discussion	
14.	School Holiday Break		
15.	Course Review		
16.	Student Learning Assessment Written Final Examination		

Course Number: SS 312 **Credit Hours:** 3

Course Title: Personality and Profiling

Required Texts

1. Canter, D., & Youngs, D. (2009). *Investigative psychology: Offender profiling and the analysis of criminal action.* Chichester, West Sussex, United Kingdom: Wiley.
2. Bloom weekly discussion notes/materials on the Blackboard system *The New York Times* or other ~~a~~lleged paper [or online products] of record proving global coverage" PsycNET [American Psychological Association]

Supplemental Texts.

a. Adams, H., & Searle, L. (2005). *Critical theory since Plato*. (3rd ed.). Boston, MA:Thomson Wadsworth.
b. Bloom, R.W. (2010). The profiler's story. *International Bulletin of Political Psychology*. http://security.pr.erau.edu.
c. Bloom, R.W. (July/August 2010). Fear of flying: Globalization, security, and terrorism.*TR NEWS*, 21-27.
d. Bloom, R. W. (2009). Assessing the dark side. [Review of the book The evaluation of child sexual abuse allegations: A comprehensive guide to assessment and testimony] *PsycCRITIQUES, 54*(29), http://www.apa.org/psyccritiques.
e. Bloom, R. W. (February 23, 2009). A government primer: What good people should know about detecting bad people. *Government Security News*, http://www.gsnmagazine.com
f. Bloom, R. W. (2007). The terrorism industry: Talking truth to power or seeking power as truth? [Review of the book The roots of terrorism.] *PsycCRITIQUES, 52*(13) *http://www.apa.org/psyccritiques*.
g. Bloom, R. W. (2006). Psychology and the law on trial. [Review of the books *Criminalprofiling: Developing an effective science and practice* and *Minds on trial*: *Great cases in law and psychology*].*PsycCRITIQUES, 51*(34),nhttp://www.apa.org/psyccritiques.
h. Bloom, R. W. (2006). Are campus law enforcement administrators ready for behaviorpattern recognition? *Campus Law Enforcement Journal, 36*(6), 17-21.
i. Bloom, R.W. (2003). Biometric, psychometric, and sociometric profiling. *International Bulletin of Political Psychology*. http://security.pr.erau.edu.

j. Bloom, R. W. (Fall 1999). Does racial profiling have a place in aviation security? *The Leader: The Magazine of Embry-Riddle Aeronautical University*.
k. Bloom, R. W. (1993). Psychological evaluations for security clearances, sensitive positions, and special access. *Military Medicine*, 519-523.
l. Bloom, R. W. (1984). Comment on 'Measuring Machiavellianism with Mach V: A psychometric investigation.' *Journal of Personality Assessment, 48*, 26-27.
m. Bloom, R. W. (1980). Comment on 'The authoritarian as measured by a personality scale Solid citizen or misfit?" *Journal of Clinical Psychology, 36*, 918-920.
n. Fox, D., & Prilleltensky, I. (1997). *Critical psychology: An introduction*. Thousand Oaks, CA: Sage.
o. Gergen, K.J. (2001). Psychological science in a postmodern context. *American Psychologist*, *56*(10), 803-813.
p. Gergen, K.J. (1985). *The social construction of the person*. New York: Springer-Verlag. Harcourt, B. E. (2007). *Against prediction: Profiling, policing, and punishing in an actuarial age.* University of Chicago Press
q. Hicks, S. J., & Sales, B.D. (2006). *Criminal profiling: Developing an effective science and practice*. Washington, DC: American Psychological Association.
r. Martin-Baro, I. (1994). *Writings for a liberation psychology*. Harvard University Press.McAdams, D.P. (2008). *The person: An introduction to the science of personality psychology. (5th ed.).* NY: Wiley.
s. Press, W.H. (2008). Strong profiling is not mathematically optimal for discovering rare

malfeasors. *Proceedings of the National Academy of Sciences*, http://www.pnas.org/content/106/6/1716.full

t) *Rare events*. (2009). McLean, VA: The MITRE Corporation: JASON Program Office. JSR-09-108

u) Sarbin, T., Carney, R.M., & C. Eoyang. (Eds.). (1994). *Citizen betrayal: Studies in trust and betrayal.* Westport, CN: Praeger.

v) Shaw, E., Ruby, K.G., & Post, J.M. (1998). The insider threat to information systems: The psychology of the dangerous insider. *Security Awareness Bulletin*, 2-98. http://www.pol-psych.com/sab.pdf

w) Tyson, L. (2006). *Critical theory today: A user-friendly guide. (2nd ed.)* NY: Routledge.

Course Description:

This course provides a rigorous and comprehensive foundation for explaining, understanding, predicting, postdicting, and influencing people. This foundation will be applied to stopping people from violating trust—viz., committing espionage—and to identifying and socially controlling them as quickly as possible after they have violated trust. The course will largely focus on personality theory and research based on scientific methodologies. The course also will explore other approaches to human knowledge and meaning including the philosophy and sociology of epistemology, literary criticism and hermeneutics, and the criticism and hermeneutics of cultural products such as film, music, dance, and painting. By course's end, students will have profiled a United States citizen convicted of spying against the United States of America.

Goals:

This is a required course for the B.S. in Global Security and Intelligence Studies program. It also is an elective course partially filling the general education requirement for upper level social sciences for all undergraduate degree programs.

Learning Outcomes: The course is designed to introduce you, the upper level student, to the role and requisites of intelligence in the contemporary world and to demonstrate an understanding of the historical, analytical, and operational parameters of intelligence. The events of 9/11/01 markedly increase the importance of this course for an understanding of threats and complexities of the international system at the outset of the twenty-first century.

1. Describing, exemplifying, critiquing, and employing major scientific personality constructs and theories [in social psychological contexts.

2. Describing, exemplifying, critiquing, and employing epistemology, literary criticism, and hermeneutics as applied to cultural products such as film, music, dance, and painting in the context of personality and personality assessment.

3. Describing, exemplifying, critiquing, and employing the formal argumentation method of profiling [in social psychological contexts.]

4. Describing, exemplifying, critiquing, and employing social deviancy theories applied to betrayals of trust.

5. Describing, exemplifying, critiquing, and employing narrative constructs and typologies of personality [in social psychological contexts.]

6. Describing, exemplifying, critiquing, and employing personnel security data, criteria, and programs [in social psychological contexts.]

Description of Assessment Activities:

Final Exam: 30%

Weekly Writing Sample: 40%

Group Project: 30%

Course Activities:

Weekly Class Structure

Relevant cultural product

Relevant article from *The New York Times* or other ~~"a~~lleged paper [or online products] of record proving global coverage"

Analysis of a scientific abstract [PsycNET]

Scientific issues from Canter & Youngs

Trans-scientific issues [Blackboard PowerPoint]

Weekly Writing Sample

The Group Project [All students in each group are expected to be able to present all aspects of project and answer all questions during presentation of project. Two initial sources are Herbig, K. L. (2008). Changes *in espionage by Americans*. Monterey, CA: Defense Personnel Security Research Center. (Technical Report 08-05)……and the Office of the National Counterintelligence Executive at http://www.ncix.gov]. Two work products are required:

Narrative Profile

Logico-Schematic Profile

Student Psychology.

Hard work, purposeful effort, common sense, creativity, and humor will take the SS312 student a long, long way. So will taking notes in class and out.…

SS 312 Personality and Profiling Lesson Plan

Week	Topic Areas	Instructional Methods	Student Assignments
1.	Introduction. Motives as Profiles	Classroom Presentation Class Discussion	Ch. 1; B #1; L1, L6, L7.
2.	History	Critiques. Student and Instructor discussions	Chs. 2-4; B #2; L2, L3, L4; L7, L8.
3.	Radex of Criminality.	Critiques. Student and Instructor discussions	Ch. 5; B#3; L1, L2, L7, L8.
4.	Radex of Criminality. .	Student and Instructor discussions Critiques	Ch. 5; B#4; L1, L2, L7, L8.
5.	Narratives of Crime	Class Discussion Critiques.	Ch. 6; B# 5; L2, L5, L7, L8.
6.	Action Patterns and Profiles	Classroom presentation and discussion Critiques.	Ch. 7; B#6; L1, L2, L5, L7, L8.
7.	Action Patterns and Profiles	Classroom presentation and discussion Critiques. Mid-Term Exam	Ch. 7; B#7; L1, L2, L5, L7, L8.
8.	Criminal Psychogeography	Class Discussion	Ch. 8; B#8; L2, L7.
9.	Basic Interviewing/Interviewing and Deception	Class Discussion Critiques.	Chs. 9-10; B #9; L1, L2, L5, L7.
10.	Acquisitive Crime/Burglary/Robbery/Fraud.	Class Discussion Critiques.	Ch. 11; B #10; L2, L7
11.	Sexual Offenses/Rape/Stalking	Class Discussion Critiques.	Ch. 12. B #11; L2, L7.
12.	Murder.	Class Discussion Critiques.	Ch. 13; B #12; L2, L7

13.	Organized Crime	Class Discussion Critiques.	Ch. 14; B #13; L2, L7.
14.	School Holiday Break		
15.	Terrorism. Final Examination Review		Ch. 15; B # 14; L2, L7.
16.	Student Learning Assessment Written Final Examination		

Appendix 1-3 Discipline Specific Courses -Security Operations Specialty Courses
These courses will provide the knowledge levels and skill sets specifically needed by an entry-level security operations management practitioner. Due the specialized nature of these courses, the course syllabi and lesson plan are provided. These courses will require normally require an experienced security practitioner as the instructor in most cases.

Course Number: SIS 395 **Credit Hours:** 3

Course Title: Security Investigations & Interviewing Techniques

Required Texts:

1. Charles & Gregory O'Hara, Fundamentals of Criminal Investigations,7th Edition, Charles C Thomas, Springfield , IL 2003
2. Zulawski & Wicklander, Practical Aspects of Interview and Interrogation, 7th Edition, CRC Press, Boca Raton, FL, 2002

Supplementary Reading Materials: Selected readings will be provided by the instructor:

a) ASIS International. Protection of Assets . Alexandria: ASIS International, (2007).
b) Vrij, A. (Detecting Lies and Deceit, Pitfalls and Opportunites, Second Edition . West Sussex: John Wiley & Sons , Ltd. (2008).
c) Martin, J. Regional Security Manager, Kinross Gold, U.S.A. Targeted Selection Interview Guide for Corporate Security Analyst Intern . Reno, NV (2010, January 18).
d) Team, J. S. (Security and Suitability Reform Proces. Washington: U.S. Government. (December 2008).
e) Department of Army. Field Manual 2-22.3, Human Intelligence Collector Operation, DOA, (September 2006)
f) Mark McClish, I Know Your Lying, The Marpa Group, Kearney, NE 2010
g) Schafer and Navarro, Advanced Interviewing Techniques; Charles C. Thomas, IL, 2003
h) FBI Law Enforcement Bulletins

Course Description: This course will focus on understanding and applying the elicitation approaches and techniques employed during security and counterintelligence investigations. The student will learn how to evaluate and investigate allegations of wrong doing objectively and systematically. The student will become familiar the various psychological approaches and behavior observation techniques used during the interview process. The students will learn to observe and read body language, behavior and other cues to help evaluate a person's truthfulness during an interview. The students will learn to plan and scope an investigation based on the legal and or regulatory elements of proof. The students will plan and conduct investigations of fictitious security violations and criminal acts including participating in mock interviews, interrogations, evidence collection, and report writing. They will also learn the Constitutional

and legal constraints and requirements involved in both general criminal and counterintelligence investigations.

Goals: Upon completion of this course, the student will be thoroughly knowledgeable of the types of investigations. Interview techniques, elicitation techniques used in security and counterintelligence investigations. The student will be familiar with the Constitutional, legal and regulatory constraints and requirements involved in both general criminal and counterintelligence investigations.

Learning Outcomes:

1. Demonstrate advanced investigative planning , interviewing and report writing skills
2. Evaluate and identify relevant information and data gathered through interviews, document reviews, and electronic databases
3. Plan and scope a security investigation including determining the necessary leads to be conducted to prove or disprove the allegation and meet the elements of proof
4. Interview witnesses and subjects in a systematic and effective manner using both direct and indirect interview techniques to elicit information
5. Demonstrate the basic knowledge of and application both inductive and deductive reasoning in investigations
6. Understand the psychological components and physiological cues that are involved in interviewing individuals
7. Be able to brief and debrief sources of criminal and intelligence information
8. Be familiar with the Constitutional and legal constraints involved in interviewing and or searching individuals suspected of crimes including espionage
9. Be able to provide clear and concise professional briefings and reports on security and criminal investigations to higher authorities

Description of Assessment Activities:

Mid-Term Examination: The examination will assess the student‘s knowledge and understanding of the fundamentals of investigations and interview techniques. The written test will consist of a combination of essay and short answer questions to test your overall knowledge and several scenarios to evaluate the student‘s understanding of the practical application of these concepts and techniques.

Final Exam: The examination will assess the student‘s comprehensive knowledge and understanding of investigations and interview techniques gained during the course and the degree

to which the student has achieved the stated learning objectives. The written test will consist of a combination of essay questions and practical scenarios to evaluate the student‘s overall knowledge and their ability to apply the knowledge in real-world scenarios.

Class Activities:

Student Exercise 1 – Review and allegation provided by the instructor and plan the investigative steps needed to resolve the allegation

Student Exercise 2 – Interview a fellow student to obtain information requested by the instructor in a lead format and draft an investigative report insert.

Student Exercise 3 – Conduct and document a subject interrogation. Instructor will provide mock suspects and the nature of the allegations.

Student Exercise 4 – Draft an investigative report from interview information, document reviews, and physical evidence provided by the instructor.

Student videotaping and Recording*:* Students enrolled in this class agree to have their interviews videotaped and recorded as directed buy the instructor.

Team Exercise: Student teams will plan and conduct an investigation to determine the facts of an alleged event through interviews, interrogations, document reviews and seizure of physical evidence. Each team will write a comprehensive investigative report and provide a formal briefing on the results of their investigation to the class. The briefing will be conducted using a power point format and all team members will be professionally dressed. The instructor will evaluate their written report and both the instructor and the class members will evaluate their presentations.

Scoring and Grading Matrix

Scoring Area	**Maximum Points**
Mid-Term Examination	25
Team Exercise 1	25
Student Exercise 1	25
Student Exercise 2	25
Student Exercise 3	25
Student Exercise 4	25
Final Examination	50

Grading
200-180 =A=100-90%
179-160= B= 89-80%
159-140= C= 79-70%

139-120=D=69-60 %
119 below=F= 59-0%

SIS 395 Security Investigations & Interview Techniques
Lesson Plan

Week	Topic Areas	Instructional Methods	Student Assignments
1.	**Course Introduction** • **Syllabus** • Methods and scope of investigations • Investigative Note taking and Report Writing	Classroom Presentation Class Discussion	Read FCI-Chapter 1,2 & 3 Student Exercise 1
2.	**Initial investigative Steps** • Elements of proof	Classroom Presentation Class Discussion	FCI-Chapter 4-7 Student Exercise 2
3.	**Basic Interview Planning and Execution** • Environment • Witness Interviews • Documentation	Class Discussion Students Practice Mock interviews	Read FCI-Chapter 8 PAII, Chapters 1 & 2
4.	**Interview Planning & Techniques** • General Approaches • Rapport building	Classroom Discussion Mock Interviews Student Interview Critiques	Read PAII, Chapter 7
5.	**Constitutional Rights & Other Legal Aspects** • US Constitutional Amendments 4,5,6& 10 • Federal Court Decisions • Right Advisement Requirements	Classroom Presentation Class Discussion	Read FCI-Chapter 9 Read PAII, Chapter 3

6.	**Confessions & Admissions** • Elicitation tactics • Miranda Warnings • False confession & admissions	Classroom presentation and discussion Video- Confessions	Read PAII-Chapters 4 &8
7.	**Identification and Interpretation of Verbal and Physical Behavior Cues** • Verbal cues • Language used, tone, speed • Non-verbal cues • Facial Micro Expressions • Body Language	Classroom presentation and discussion Practical observations of interview subjects	READ PAII-Chapter 5
8.	**Accusation Credibility** • Testing Complaint • Source creditability • Corroborating complainant‘s account	Classroom presentation and discussion Mock Interviews	Read FCI-Chapter 9
9.	**Mid- Term Review & Examination** • Basic Security Concepts & Applications • Post Examination Review	Written questions and practical scenarios	Read Handouts Assignment of Team Projects
10.	**Rationalizations** • Identify • Learn to employ	Classroom discussion Mock Interviews	PAII, Chapter 10
11.	**Denials** • Types • Overcoming denials • Corroborating information	Student Exercise 3	PAII, Chapter 11

12.	**Practice Statement Taking** • Verbal and written • Voluntary w/o coercion • Content • Authorship • Sworn and unsworn	Mock Interviews	
13.	**Team Interviews** • Witness Interviews • Subject interviews • Report inserts and notes	Team Exercise	Out of class activity Interview mock witnesses and subjects
14.	Taking Statements & Recording Interviews	Student Exercise 4	Read PAII, Chapter 14 FCI, Chapter 10
15.	Specialized Interviewing		Read PAII, Chapter 18
16.	**Course Review & Student Learning Assessment** c) Comprehensive Course Review d) Written Final Examination	Written questions and practical application scenarios	

Course Number: SIS 4XX **Credit Hours:** 3

Course Title: Government Security Operations and Management

Required Texts:

1. Charles Sennewald, Effective Security Management ,5th Edition, Elsevier Charles C Thomas, Springfield , IL 2011
2. Dr. Gerald L. Kovacich, The Information Systems Security Officer's Guide, 2nd Edition, Butterworth/Heinemann, (2003)
3. National Security Industrial Program Manual , U.S. Government (current)
4. *Federal Investigative Standards*, U.S. Office of Personnel Management , Dec 13, 2008
5. *An Overview of the United States Intelligence Community for the 111th Congress, U.S. Government, (2009)*
6. *Milton D. Rosenau, Jr., Successful Project Management, 3rd Edition, John Wiley and Sons, NY, (1998)*

Course Description: This course will focus on understanding the federal intelligence and security organizations, their organizational structure, responsibilities and functions. This course will stress the pivotal role the federal security officer plays in these organizations in the protection of personnel, assets, and information. The student will learn the critical importance of personnel screening and information protection in preventing espionage and other crimes. The student will draft security plans and policies in these critical areas. The student will learn how to apply personnel policies involving the hiring, evaluation and termination of employees. They will recognize ~~"re~~d flags" in the hiring process and the possibility of workplace violence resulting from terminations. Students will develop and practice briefing employees and senior executives on security awareness issues including counterintelligence threats. Throughout the course, individual students and student teams will be challenged to make decisions under time pressures without complete information affecting organizational security and operations

Goals: Upon completion of this course, the student will understand the critical role that a federal security officer plays in protecting people, facilities, and information in the government. He will be able to draft security plans and policies for government and private organizations. The student will have the knowledge, analytical capabilities, and skill sets necessary for an entry-level security manager in both government and private organizations.

Learning Outcomes:

1. Understand the federal intelligence and security organizations, their organizational structure, responsibilities, and functions as well as understand the functional areas in both government and private industry such as personnel, finance and operations

2. Understand the interrelationships between these functional entities and the associated government regulatory requirements

3. Understand the federal government budgeting process and how it may be impacted by budget rules and policy decisions

4. Draft security policies and procedures to implement regulatory requirements

5. Be familiar with government personnel polices related to hiring, evaluating and terminating employees

6. Be able to develop and present effective security awareness briefing to employees and senior managers

7. Prepare and execute physical security plans that meet or exceed federal requirements

8. Make sound decisions based on security knowledge and skill sets learned under time pressures

9. Understand and apply government information security requirements to protect classified documents, communications and computer networks from unauthorized access and or damage

10. Produce professional (individual and group) quality reports and presentations.

Description of Assessment Activities:

Mid-Term Examination*:* The examination will assess the student‘s knowledge and understanding of federal intelligence and security organizations, personnel management, basic security concepts, security organization and management, legal issues, risk management and threat assessment, physical security concepts and equipment, and personnel security measures. The written test will consist of a combination of essay and short answer questions to test their overall knowledge and several scenarios to evaluate the student‘s understanding of the practical application of these concepts and techniques.

Final Exam: The examination will assess the student‘s comprehensive knowledge and ability to apply security concepts and principles, risk management and threat assessment, physical security concepts and equipment, and personnel security measures, emergency and contingency planning in government facilities. , workplace violence, information and computer security The written test will consist of a combination of essay questions and practical scenarios to evaluate the student‘s overall knowledge and their ability to apply the knowledge in real-world scenarios.

Class Activities:

Individual Exercise 1- Draft a workplace policy and procedure for their team’s organization. This exercise is designed to allow the individual student to apply concepts and principles learned in a practical manner and to allow students to practice policy and procedure writing skills. The instructor will evaluate and provide feedback to the individual student.

Individual Exercise 2 – Draft a basic information security policy to ensure employee awareness and protection of company sensitive or government classified material. This exercise is designed to allow the individual student to apply information security concepts and principles learned in a practical manner and to allow students to practice policy and procedure writing skills the instructor will evaluate and provide feedback to the individual student.

Team Exercise 1 – Organize and staff a proposed security department for the fictitious organization along with developing the supporting department expense budget. The team must determine the most effective reporting level for the senior security manager, the titles, and functions of his or her subordinates and their proposed locations within the organization. The instructor will review and evaluate each team‘s proposed security organization and provide feedback.

Team Exercise 2 – Conduct a risk management assessment of a newly proposed government facility in a foreign country. The team must apply a risk assessment model to identify all the hazards, determine their likelihood, the vulnerabilities of the faculty and the criticality to the faculty should such an event occur. Brief the class and instructor on their risk assessment and priority resource allocation.

Team Exercise 3 – Identify and select the most effective security equipment to purchase and install in the new facility. The team must identify, select, and cost out all of the equipment that believe to be warranted by the threats identified. They must also develop a capital budget for the new facility. The team must brief the instructor and their classmates of their results with a formal power point presentation**.**

Scoring and Grading Matrix

Scoring Area	**Maximum Points**
Mid-Term Examination	50
Team Exercise 1	25
Team Exercise 2	25
Student Exercise 1	25
Student Exercise 3	25
Final Examination	50

Grading
200-180 =A=100-90%
179-160= B= 89-80%
159-140= C= 79-70%
139-120=D=69-60 %
119 below=F= 59-0%

SIS 4XX Government Security Operations and Management Lesson Plan

Week	**Topic Areas**	**Instructional Methods**	**Student Assignments**
1.	**Role & Functions of Federal Security Officers** • Course Introduction • IC Organizations	Classroom Presentation Class Discussion	Visit DNI Website Read Required Article 5 NISPOM, Section 2, general Requirements
2.	**General Security Management** • Principles of organization • Organizational Structure • Security‘s Role in the Organization		ESM Chapters 1-6

	• The security manager and staff		
3.	**Personnel Management Practices** • Hiring & Selection • Background investigations • Federal standards • Job Descriptions • Promotion polices • Disciplinary polices	Complete SF 86 and Contractor Employee Applications	ESM Chapters 7,8,10 and 12 Required Article 4 NISPOM, Chapter 2
4.	**General and Security Employee Training** • New employee • Recurrent • Special • On-Job-Training • On-line Security Training • Security Procedures • Equipment Operations • Information Protection Issues		Defense Security Website (STEMS) ASIS International Website NISPOM, Chapter 3 ESM Chapter 9
5.	**Planning and Budgeting** • How is a budget prepared? • Historic v. Zero-Based • Personnel budgeting • Capital budgeting • Expense Budgeting • Budget justifications • Constructing and Defending the Department Budget		ESM, Chapter 15
6.	**Risk Management & Threat Identification** • General Approaches to Risk Management • Threat Identification • Risk management modeling • R=Threat Vulnerability+ Criticality + Likelihood	Classroom Presentation Class Discussion	ESM Chapter 17

7.	**Threat Assessments** • Threat Assessment Models • Threat Levels • Vulnerability factors • Criticality • Threat Assessment Matrix • Risk Assessment Teams	Threat Assessment Demonstration	Student Exercise 1- Conduct Faculty Threat Assessment
8.	**Project Management** • Definition • Process • Planning • Project Deliverables • Project Team • PM Software **Mid-Term Examination**	Classroom Presentation Demonstration of Microsoft Project Set Up Begin Team Project	ESM Chapter 16 Read SPM Student Exercise 2- Set Up Project using MS Project
9.	**Spring or Fall Break- No Classes**		
10.	**Information Protection** • Safeguarding Classified information • Security-related information • CI threats	Case studies	NISPOM, Chap. 5 ESM Chapter 21 ISSO, Section II DNI website-CI Executive
11.	**Team Projects** • Team Project Meetings • Team Project Presentations • Peer Review Sessions •	Classroom Presentation Class Discussion	
12.	**Integration of Security & Other Systems** • Alarm ,CCTV, IT • Security alarm and surveillance monitoring • On-site verses off –site monitoring		Technical data sheets
13.	**Emergency Operations & Response** • Security Response • Emergency Evacuation	Classroom discussion Video	Student Exercise 4- Draft an emergency evacuation plan

	• Bomb Threat • Contingency Planning • Crisis management		
14.	**Conducting and Managing Investigations** • Security investigations scope and format • Background Investigations • Developing security investigation documentation • Evidence collection • Case management	Classroom Presentation	Handouts
15.	Comprehensive Course Review		
16.	**Student Learning Assessment** • Scenario Evaluation • Written Final Examination		

Course Number: SIS 422 **Credit Hours**: 3

Course Title: Homeland Security and Technologies

Required Texts:

1. Nemeth, Charles P. Homeland Security, An Introduction to Principles and Practices , CRC Press ,Boca Raton, FL, 2010
2. Supplemental readings provided to students in this class;
    a. 911 Commission Report

Course Description: This course provides an overview of the homeland security effort in the United States, the evolution of homeland security from the fields of traditional civil defense and emergency preparedness and the development of the Department of Homeland Security. During the course, the need to understand the individual roles of the federal and state governments and the collaborative nature of their coordinated efforts in supporting homeland security will be explored. The students will also be familiarized with the National Strategy for Homeland Security; the creation, organizational development, and functions of the U.S. Department of

Homeland Security; the National Response Plan; the National Incident Management System and the technological resources supporting the homeland security mission.

Goals: Upon completion of SIS 422, the student should be equipped with the knowledge and analytical skills necessary to participate in the homeland security effort both as a private citizen and security professional. The student should have good understanding of the broad scope and impact of homeland security on the government, the private sector, and the public; the evolution and organization of the U.S. Department of Homeland Security; and the technologies supporting this effort.

Learning Outcomes:

1. Demonstrate a general knowledge of the historical development of homeland security.
2. Understand the development, organization, and mission of the U.S. Department of Homeland Security (DHS).
3. Understand the roles and interdependency of federal, state and local government in responding and mitigating disasters including those resulting from terror-related incidents.
4. Demonstrate the capacity to use analytical methodologies to evaluate threats to industrial sectors and suggest appropriate mitigation strategies
5. Be familiar with the technologies employed in support of homeland security
6. Effectively critique and participate in citizen and government discussions of homeland security issues
7. Be familiar with the National Response Framework & the National Incident Management System
8. Produce professional (individual and group) quality reports and presentations.

Assessment and Evaluation:

Assessment Items	**Maximum Points**
Quizzes (3 x 25 pts. each)	75
Team Practical Project	100
Individual Research Paper	50

Final Written Examination	75
Total Assessment Score	300

Description of Assessment Activities

Quizzes: There will be three (3) quizzes based on readings and class lectures. They are intended to help you understand the reading and key concepts in preparation for your presentations and final exam. Quizzes that are missed may be taken later with the instructor approval.

Sector Review & Presentation: Student teams will research a particular public or private sector to understand the scope, critically, and vulnerability of the sector to attack. Sectors include transportation, information networks, utilities, etc. The students will also recommend mitigation actions. Prior instructor approval of topic required to avoid duplication. A power point presentation of findings to the class is required.

Research Paper: An individual research paper is required. The paper shall be a minimum of 8 pages not including the front page and reference page with at least 6 references. Authoritative, reliable references are required. Use the APA format in developing your paper and citing references. Additional information on the term paper topics and format will be provided by the instructor. The score on papers turned in prior to required date will be increased by 5 points. No late papers will be accepted.

Final Exam: The exam will be comprehensive and include both an essay and short answer questions to test your overall knowledge and understanding of the concepts and principles of homeland security, their application during emergency events, and the application of supporting technologies.

Class Policies *Vary based on university requirements and instructor preference.*

SIS 422 Homeland Security and Technologies Lesson Plan

Legend; Homeland Security: An Introduction to Principles and Practices= ***HSIPPP***

Week	Topic Areas	Instructional Methods	Student Assignments
1	**Course Introduction & Overview** • Homeland Defense & Security • DHS History & Establishment	Classroom Presentation Class Discussion	HSIPPP, Read Chapter 1 Visit DHS website

2	**911 Attack & aftermath** • 911 attack details • 911 Commission findings • 911 Commission recommendations	911 Commission Video Discussion	Read selections from 911 commission Report HSIPPP. Read Chapter 2
3	**DHS Establishment** • Statutory Authorities • DHS Organization and Structure • DHS Budget & Funding	Classroom Presentation Class Discussion Quiz 1	HSIPPP, Read Chapter 3
4	**Risk Management** • Concepts • General Approaches to Risk Management • Threat Identification • Natural and Manmade	Class Discussion Practical Threat Assessment Exercise Team Project 2	HSIPPP, Read Chapter 4
5	**DHS Agencies & CI Protection** • DHS Agency Profiles • Critical Infrastructure Protection	Classroom Presentation Class Discussion	DHS Critical Information Protection Plan (CIPP)
6	**Cyber security** • Component of CI • National Cyber Security Div. • U.S. CERT	Classroom presentation and discussion Quiz 2	HSIPPP, Read Chapter 4 Section 4.4
7	**Sector Security** • Border Security - Preventing Illegal Immigration • Transportation security	Classroom presentation and discussion Video	HSIPPP, Read Chapter 9,10
8	**Emergency Management** • All Hazards Approach • DHS/FEMA • NIMS Incident Command System- IC System • Emergency Operations Center	Classroom discussion & discussion Practical table top exercises	HSIPPP, Read Chapter 5 & 7
9	**Mid- Term** • Review • Examination	Classroom discussion Written Examination	
10	**Weapons of Mass Destruction**	Classroom discussion Video	HSIPPP, Read Chapter 4

	• Chemical • Biological • Nuclear	Case Study Anthrax Attack	Section 4.3.2
11	**State & Local Homeland Security Organizations** • Arizona State • Arizona Counter Terrorism Information Center		HSIPPP, Read Chapter 6
12	**US Intelligence Community** • FBI • CIA • DNI	Quiz 3	HSIPPP, Read Chapter 8
13	**Team Projects** • Team Project Meetings • Team Project Presentations • Peer Review Sessions		
14	**Homeland Security & Public Health** • Roles & functions • Water • Agriculture and food • Pandemic Threats		HSIPPP, Read Chapter 11
15	• DHS Future • Comprehensive Course Review		HSIPPP, Read Chapter 12 Research Paper Due
16	**Student Learning Assessment** • Comprehensive written examination		

Course Number: SIS 4XX **Credit Hours: 3**

Course Title: Physical Security and Facility Design

Required Texts:

1. David D. Owen & RS Means Engineering Staff, Building Security: Strategies & Costs, Construction; Publishers & Consultants, Kingston, MA, USA(2003)

2. David G. Patterson, Implementing Physical Protection Systems; A Practical Guide, ASIS International, Arlington, VA (2004
3. Supplementary Readings: Reading assignments and reference items provided by instructor.
    c) ASIS International. (2007). Protection of Assets . Alexandria: ASIS International
    d) U.S. Department of Army, Field Manual 3-19.30, Pysical Security , DOA, January 8, 2001
    e) Director of Central Intelligence Directive 6/9, Physical Security Standards for Sensitive Compartmented Information Facilities (Nov 18, 2002)

Course Description: This course will focus on understanding and applying physical security concepts and principles to protect people, information, and facilities against criminal activities and terrorist attacks. The students will learn the basic security concepts underlying such protective activities, the types of physical security measures and equipment that may be employed, and their effectiveness in terms of threat mitigation and cost. The students will become familiar with integrating security into the facility planning process, blueprint reading, and equipment selection based on threat assessment and facility use. Student teams will review building designs for security effectiveness and conduct security audits of existing buildings. The teams will also be responsible for physical security measures and equipment to be chosen in designing for retrofitting a major government or private facility. This project will include evaluating the security needs based on the facility‘s proposed operations, personnel staffing, and assets, including the development of a capital budget

Goals: Upon completion of this course, the student should have the knowledge and analytical skills necessary to participate in security planning to protect personnel, information, and facilities. The student will be familiar with risk management principles, facility security strategies and costs, and the practical application of these principles and strategies

Learning Outcomes:

1. Demonstrate physical security theory in their decision making

2. Understand the basic principles of facility construction including: blueprint interpretation, specification development, cost strategies, and construction inspection and review processes

3. Ability to develop, prepare, and execute physical security plans

4. Ability to perform physical security surveys and inspections

5. Ability to create multilayered security systems involving access controls, barriers, protective devices, monitoring equipment, security forces, and intrusion devices

6. Understand principles of physical security hardware, the systems approach to security, and integration of basic life safety codes and ADA requirements

7. Understand the physical security measures that are available for protecting classified information in the form of documents and electronic data

8. Ability to evaluate and apply new or advanced security technologies and equipment to protect government personnel, information, and facilities

9. Be able to provide professional briefings and written reports on course-related subject matter

Student Assessment Activities

Mid-Term Written Examination	100
Team Exercise	100
Individual Exercise 1	25
Individual Exercise 2	25
Individual Exercise 3	25
Individual Exercise 4	25
Final Written Examination	100
Total Assessment Score	400

Description of Assessment Activities

Team Exercise 1- Conduct and Report the Results of a Facility Threat Assessment

This team exercise will require the team to review simulated intelligence information and hazard information, apply the information to a general risk assessment model (identifying threat levels, vulnerabilities and criticality of the faculty) and determine the various levels of risk and the appropriate mitigation approach. Brief the class and instructor on their threat assessment results and rationale.

Team Exercise 2-.Organize a project team and develop a project plan using Microsoft project. The instructor will assign class members to specific teams. Each team will be responsible for selecting their leadership and alignment of duties along with developing an initial project plan using Microsoft Project. The instructor will review and evaluate each team‘s proposed project team organization and plan and provide feedback.

Team Exercise 3- Review mock faculty blueprints and determine most effective physical security equipment to be employed to protect the facility and its perimeter. Brief the class and instructor on their equipment selections, locations and selection rationale.

Team Exercise 4- Develop both a capital and expense project budget for the new or renovated faculty. Using the information developed in previous exercises, the team will cost out the equipment options chosen, the cost of security employees or contractors needed to complete the project, etc. Brief the class and instructor on their proposed budgets.

Student Exercise 1- Draft an emergency evacuation policy and procedure for a faculty designated by the instructor. This exercise is designed to allow the individual student to apply concepts and principles learned in a practical manner and to allow students to practice policy and procedure writing skills. The instructor will evaluate and provide feedback to the individual student.

Student Exercise 2 – Draft the specifications for a Request for Proposal for Contract Security Officer Service. Write memo to the facility manager supporting the proposed contract service RFP. The instructor will evaluate and provide feedback to the individual student.

Mid-Term Examination: The examination will assess the student‘s knowledge and understanding of the risk management and threat assessment, project management and planning, security design and equipment specifications. The written test will consist of a combination of essay and short answer questions to test your overall knowledge and several scenarios to evaluate the student‘s understanding of the practical application of these concepts and techniques.

Final Exam: The examination will assess the student‘s comprehensive knowledge and understanding of security concepts and principles, risk management and threat assessment, project management and planning, security design and equipment applications, emergency operations and response, systems integration, budgeting and vendor selection and security training. The written test will consist of a combination of essay questions and practical scenarios to evaluate the student‘s overall knowledge and their ability to apply the knowledge in real-world scenarios.

Class Policies *Vary based on university requirements and instructor preference.*

SIS 4XX Physical Security and Facility Design Lesson Plan

Legend: Building Security Strategies & Costs **= BSSC**
Implementing Physical Protection Systems: A Practical Guide = **IPPS**

Week	Topic Areas	Instructional Methods	Student Assignments
1	**People, Property, Security and Safety**	Classroom	BSSC Chapter 1 IPPS Chapter 1

	• Course Introduction • General Security Areas • Physical, Personnel, Information • Security and Safety Conflicts	Presentation Class Discussion	
2	**Risk Management & Threat Identification** • General Approaches to Risk Management • Threat Identification • Natural and Manmade	Classroom Presentation Class Discussion	BSSC Chapter 2 IPPS, Chapter 2
3	**Threat Assessments** • Threat Assessments • Threat Levels • Vulnerability factors • Criticality • Threat Assessment Matrix • Risk Assessment Teams	Threat Assessment Demonstration	BSSC Chapter 3 Team Exercise 1- Conduct Faculty Threat Assessment
4	**Project Management** • Definition • Process • Planning • Project stages • Project Deliverables • Project Team • PM Software	Classroom Presentation Demonstration of Microsoft Project Set Up	IPPS, Chapter 3 Student Exercise 2- Set Up Project using MS Project Team Exercise 4
5	**Planning** • Project Team • Requirements • Stakeholders • System Design • Blueprint familiarity • Cost Estimates	Class Discussion Practical Blueprint Reading Exercise Team Assignments	IPPS, Chapter 4 Team Assignments
6	**Security Through Design** • Approaches to Physical Security • Area and Perimeter Security • Points of Ingress & Egress • Interior Space Protection • Fire & Safety Concerns	Classroom presentation and discussion Fire Exit Controls Ingress & Egress Security Devices	BSSC Chapter 5 IPPS, Chapter 5 Team Exercise 3- Ingress Design

7	**Security Devices & Systems** Security Systems Concept Fencing and Gates Lighting CCTV surveillance Intrusion Detection Systems Security Personnel & Patrols Security Operations Center	Discussion and review of technical requirements and specifications of security systems and devices	BSSC Chapter 8
8	**Emergency Operations & Response** • Security Response • Emergency Evacuation • Bomb Threat • Contingency Planning • Crisis management	Classroom discussion Video	BSSC Chapter 4 & 7 Student Exercise 1- Draft an emergency evacuation plan
9	**Integration of Security & Other Systems** • Information Security • Security alarm and surveillance monitoring • On-site verses off –site monitoring	Classroom discussion Sensitive Compartmented Information Facilities	BSSC Chapter 9 Directive 6/9,
10	**Project Cost Estimation & Budgeting** • Types of cost estimates • Life Cycle Cost • Capital Budgeting • Expense Budgeting • Project Budgeting software	Classroom Demonstration Budgeting Practice Exercises	BSSC , Part 2 IPPS, Chapter 6
11	**Contractor & Vendor Selection** • Procurement approaches • Request for Proposal (RFP) • Specifications • Evaluation Criteria • Selection process		IPPS, Chapter 7 Student Exercise 2
12	**Team Projects** • Team Project Presentations • Peer Review Sessions		Team Exercises 2,3 and 4
13	**Team Projects** • Team Project Presentations		Team Exercises 2,3 and 4

	• Peer Review Sessions		
14	**System & equipment Installation** System and component planning System tuning Systems Maintenance issues		IPPS, Chapter 8
15	Security & Employee Training Security Procedures Equipment Operations Information Protection Issues High Rise Protection Issues		IPPS, Chapter 9
16	Course Review & Student Learning Assessment Comprehensive Course Review Written Final Examination		

Course Number: SIS 4XX **Credit Hours**: 3

Title: Security Operations Management Practicum

Required Texts:

1. Charles A. Senewald, Effective Security Management , Elsevier
2. David G. Patterson, Implementing Physical Protection Systems; A Practical Guide, ASIS International, Arlington, VA (2004
3. U.S. Department of Army, Field Manual 3-19.30, Pysical Security , DOA, January 8, 2001
4. Director of Central Intelligence Directive 6/9, Physical Security Standards for Sensitive Compartmented Information Facilities (Nov 18, 2002)
5. Charles & Gregory O'Hara, Fundamentals of Criminal Investigations,7th Edition, Charles C Thomas, Springfield , IL 2003
6. National Industrial Security Manual(current)
7. Federal Investigative Guidelines, U.S. Office of Personnel Management , Dec 13, 2008

Course Description: This course will draw on the knowledge and skill sets that the student has obtained throughout their course study in security operations through practicum based role-play and security scenarios. The students will act as Program Security Officers, Information System Security Officers, and Facility Security Officers (National Industrial Security Program). The students will practice performing government clearance procedures for personnel and facilities including prescreening applicants, using government databases, and briefing and debriefing government and contractor employees. The students will also role-play interaction with a variety of day-to-day personnel security issues, involving security inspection audit deficiencies and

corrections, security violation investigations, and classified information loss or unauthorized disclosure.

Goals: Upon completion of this course, the student will be knowledgeable and familiar with the various roles and responsibilities of a government security officer. The student will also be familiar with the appropriate government security regulations, databases, and security investigation techniques.

Learning Outcomes: Upon course completion, students will be able to:

1. Understand the scope and variety of responsibilities of a government security officer.
2. Demonstrate their ability to apply their knowledge of security operations in a real world environment
3. Demonstrate their familiarity with the U.S. government security clearance processes
4. Understand the roles and interdependency of federal, state, and local government in responding to and mitigating disasters including those resulting from terror-related incidents
5. Evaluate security threats to government operations, personnel, and facilities and recommend mitigation strategies
6. Be familiar with security investigation methodologies and interviewing techniques
7. Effectively critique and participate in government and industry discussions of personnel and facility security issues
8. Be familiar with the DOD Security Classification System and the National Industrial Security Program
9. Be able to conduct professional briefings and write investigative reports in course-related subject matter

Student Assessment Activities

Team Exercise 1	25
Team Exercise 2	25
Team Exercise 3	25
Team Exercise 4	25
Individual Exercise 1	50

Individual Exercise 2	50
Final Written Examination	100
Total Assessment Score	300

Note: Individual & team scores are totaled to arrive at your final course score

300-270 = A
269-240 =B
239-210=C
209-180=D
179 –below F

Description of Assessment Activities

Team Exercise 1-. Determine their eligibility for the necessary clearance levels by applying the investigative results to the federal government‘ guidelines for adjudication. Review the results of background investigations on several new government employees who will need different levels of access to sensitive and classified information in their jobs

Team Exercise 2- Determine the physical security requirements necessary for establishing a Sensitive Compartmented Information Facility.

Team Exercise 3- Determine the necessary security requirements to be met by a fictitious company that has received a U.S. government contract involving access to secret information.

Team Exercise 4- Conduct an investigation on the loss or compromise of government classified information at your facility. You are to construct the scope of the investigation, interview those involved, collect and review and relevant documents, and provide a narrative report of your results.

Student Exercise 1- Draft an emergency evacuation policy and procedure for a faculty designated by the instructor. This exercise is designed to allow the individual student to apply concepts and principles learned in a practical manner and to allow students to practice policy and procedure writing skills. The instructor will evaluate and provide feedback to the individual student.

Student Exercise 2 – Brief the CEO on the NISP purpose and requirements. This will be an executive-level briefing using 10 power point slides or less

Final Exam: The examination will assess the student‘s comprehensive knowledge and understanding of the federal security officer‘s role and functions in government and private organizations, the National Industrial Security Program, the federal government security classification and clearance processes, applying security principles and concepts in practical

scenarios and readiness for an entry-level security officer's position in the federal government The written test will consist of a combination of essay questions and practical scenarios to evaluate the student's overall knowledge and their ability to apply the knowledge in real-world scenarios.

4XX **Security Operations Management Practicum Lesson Plan**

Legend: Effective Security Management = **ESM**
Federal Information Security Manager = **FISM**

Weeks	**Topic Areas**	**Instructional Methods**	**Student Assignments**
1-3	**Security Concept and Principles review**	Classroom Presentation Class Discussion Comprehensive Written Examination	
4-5	**Team Exercise 1- Perform a threat Assessment of a government facility located in a foreign country**	Classroom Presentation Class Discussion	Country studies Facility review Intelligence analysis
6-7	**Team Exercise 2-** Determine the physical security requirements necessary for establishing a Sensitive Compartmented Information facility. •	Threat Assessment Demonstration	Student Exercise 1- Conduct Faculty Threat Assessment
8-9	**Team Exercise 3-** Determine the necessary security requirements to be met by a fictitious company that has received a U.S. government contract involving access to secret information. **Planning**	Classroom Presentation Demonstration of Microsoft Project Set Up	Student Exercise 2- Set Up Project using MS Project
10-11	• **Integration of Security & Other Conduct** an investigation on the loss or compromise of government classified information at your	Class Discussion Practical Blueprint Reading Exercise Team Assignments	Team Assignments

	facility. You are to construct the scope of the investigation, interview those involved, collect and review and relevant documents, and provide a narrative report of your results		
12-13 14-15	**Security Through Design** • Approaches to Physical Security • Area and Perimeter Security • Points of Ingress & Egress • Interior Space Protection • Fire & Safety Concerns	Classroom presentation and discussion Fire Exit Controls Ingress & Egress Security Devices	
16	**S** Course Review & Student Learning Assessment Comprehensive Course Review Written Final Examination		

Course Number: SIS 425

Course Title: Information Protection and Computer Security **Credit Hours:** 3

Required Texts:

1. Michael G. Solomon & Mike Chapple, Information Security Illuminated, Jones & Bartlett, Sudbury, MA 2005
2. Mark Osborne, How to Cheat At Managing Information Security, Syngress Publishing, Inc., MA 2006

Course Description: This course provides students with a familiarity with information protection programs in both the government and private sectors. The course also provides the students with an overview of computer security including physical security practices, hardware and software protection. Students will learn the importance of applying proper security protection measures to classified and sensitive information to prevent its intentional or unintentional unauthorized disclosure. Students will review the U.S. government‘s regulatory scheme for protection of its classified information including several case studies of unlawful information disclosure. Similarly, the students will review information protection practices in private organizations and their importance. Students will examine and discuss the various aspects

of computer security including physical protection of hardware, software protective programs and employee security awareness programs. The students will also learn how to detect and investigation computer crimes.

Goals: Upon completion of SIS 425, the student should have good understanding of the broad scope of information protection and the types of protection available for computer systems. The student will learn the basic principles of a good information security program. The student will also learn the basic concepts of computer security involving physical access control and software and hardware protection. This information will allow the student to recognize the importance of information security and computer security applications in both the government and private sectors.

Learning Outcomes:

1. Understand the critical need to protect sensitive information both in government and private organizations.
2. Demonstrate the ability to develop and write a basic information security program
3. Understand general security principles and practices as they apply to sensitive information and computerized systems
4. Understand basic computer and network security concepts
5. Be familiar with operating system security measures
6. Be knowledgeable of computer security tools and software
7. Be familiar with cryptographic technologies used in message transmission
8. Produce professional (individual and group) quality reports and presentations.

Assessment and Evaluation:

Assessment Items	**Maximum Points**
Mid-Term Written Examination	100
Team Practical Project	100
Individual Practical Project (2) @ 25 each	50
Defense Security Service Course (2)	50
Final Written Examination	100

Total Assessment Score	400

Description of Assessment Activities

Individual Knowledge Application Exercises - These are practical scenarios that require the individual to apply his or her information and computer security knowledge in practical scenarios. Each scenario is worth 10 points.

Team Exercise & Presentation: Draft the information protection and computer security policy for a government or private business organization. The team will be task with writing various security policies and procedures for their organization. Teams will be evaluated on the thoroughness of their proposed security programs, the clarity and quality of their assigned policies and procedures. Their presentation must provide a general overview of their chosen organization, details of their proposed security plan, and a discussion of the security policies and procedures that they wrote. Presentations should last 15-20 minutes. Students are to wear business attire. The team will present their findings to the class using Power Point. The use of graphics, video clips, photographs, or props to support your presentation are encouraged. At the conclusion of your presentation, you must provide a copy of your presentation including a bibliography identifying the sources that you used in developing your presentation. Team presentation evaluation will include quality of the presentation, supporting research, team member participation, professional manner and dress. Peer evaluations will be included in the overall evaluation. All team members will receive the same score unless they have not significantly participated in the research effort or the presentation as determined by their team mates and the instructor.

Completion of two on-line Defense Security Service Courses. The instructor will select the course to complement the course and enhance the student‘s understanding of the role and functions of a federal security officer in protecting classified government security.

Mid-Term Exam: The examination will combine both survey and essay type questions to test your overall knowledge and understanding of information protection and computer security concepts and applications discussed in the course to date.

Final Exam: The exam will be a combination of essays and short answer questions to test your overall knowledge and understanding of the concepts and principles of information protection and computer security and their application in practice

Class Policies *Vary based on university requirements and instructor preference.*

SIS 425 Information Protection and Computer Security Lesson Plan

Week	Topic Areas	Instructional Methods	Student Assignments
1	**Information Security Policy** • Course Introduction Syllabus Discussion • Information Security Organization • Policy Development	Classroom Presentation Class Discussion	MIS, Chapter 1,2
2	**Information Security** • Concepts • Principles • Jargon	View and Discuss Wiki Leaks Video	MIS, Chapter 3 ISL, Chapter 1 & 3
3	**Laws and Regulations** • Information Security Laws & Regulations • U.S. Government Information Security		MIS –Chapter 4 ILS Chapter 4
4	**U.S. Government Information Security** • CI & Espionage case studies • Background Investigations scope • Background Investigations adjudication procedures	Video Spies Among Us Classroom discussion Practical exercises	Handouts
5	• National Industrial Security Program • CI Case Studies	Cyber Crimes Video Classroom Presentation and Discussions	
6	• Business Security • Competitive Intelligence	Classroom presentation and discussion	MIS, Chapter 4 ILS, Chapter 4
7	Secure TCP/IP • Components • TCP Packet Construction •		ILS Chapter 6
8	Mid Term Course Review Mid-Term Examination		

9	• Access Control Methodologies • Cryptographic Technologies • Securing Operating Systems	Classroom discussion	ILS , Chapter 2, 5
10	Network & Server Attacks and Penetration Security Auditing Intrusion Detection Systems and Practices	Classroom discussion	ILS, Chapter 12 MIS, Chapter 12 ILS, Chapter 11 ILS, Chapter 13 MIS, Chapter 9
11	Security Incidents Investigation of security incidents		ILS, Chapter 7
12	• Security System Scanning • Infrastructure Security		ILS, Chapter 14 MIS, Chapter 7
13	Team Projects • Team Project Meetings • Team Presentations • Peer Review Sessions		
14	Team Projects • Team Project Meetings • Team Presentations • Peer Review Sessions		
15	Application Security Flaws and Testing Comprehensive Course Review		MIS, Chapter 13
16	Course Review & Student Learning Assessment Written Final Examination		

Course Number: SIS 410 **Credit Hours**: 3

Course Title: Corporate Security Operations and Management

Required Texts:

1. John Jay Fay, Contemporary Security Management , 3nd Edition, Elsevier Butterworth-Heinemann, Burlington, MA 2011

Course Description: This course will focus on the management of security private companies and corporations, both in the domestic and international arenas. The course will familiarize the students with the security threats facing both domestic and international businesses and the new post-911 security challenges. Among the topics addressed are personnel security, physical security, information security, investigations, executive protection and crisis and emergency planning and response. In addition to address these topics, the course will explore the use of competitive intelligence in the business world. This exploration will include the use of legal intelligence collection methods including open sources to identify new business opportunities and products, to determine the strategic marketing and financial plans of a competitor, and to reverse engineer a competitor‘s products. Finally, the course will review the professional, legal and ethical issues that influence the implementation of various security measures and competitive intelligence operations.

Goals: This is a required core course in the SIS program. The goal of the course is to give the student a real world perspective of what management and operational issues professionals in the corporate security organizations face and what measures they take to resolve these issues. After completing this course, the student will be familiar with the security threats facing both domestic and international businesses, the role of corporate security managers in evaluating and mitigating such threats, and the new post-911 security challenges. The student will also understand the legal, ethical and professional obligations assumed by a corporate security manager for their performance in protecting company employees, facilities, and sensitive information. A student who successfully completes this course would have a significant advantage in interviewing with major domestic and international corporations seeking persons for corporate security positions.

Learning Outcomes:

1. Understand the pivotal role of security in the corporate organization and in the overall success of the business mission.

2. Be aware of the impact of the security on the overall effectiveness, financial well-being and success of businesses both domestic and international.

3. Understand the principles of good management and leadership in the security profession.

4. Be familiar with the various types of security equipment, their effectiveness, and cost benefit to the corporation.

5. Understand the nature and scope of the threats faced by businesses from their employees, competitors, customers, contractors, and terrorists.

6. Perform elementary security risk assessments of various business operations to evaluate the level of the threat, identify security countermeasures, and allocate the necessary company resources.

7. Understand the importance of protecting information from competitors; while legally collecting such information on competitors.

8. Be aware of the government regulatory oversight of security practices in many industrial sectors.

9. Appreciate the importance of social, political, cultural, and psychological dimensions in approaching a security threat and resolving it in an effective manner.

10. Produce professional (individual and group) quality reports and presentations.

Assessment and Evaluation:

Assessment Items	**Maximum Points**
Quizzes (2 x 50 pts. each)	100
Team Practical Project	100
Final Written Examination	100
Total Assessment Score	300

Description of Assessment Activities

Quizzes: There will be based on readings and class lectures. They are intended to help you understand the reading and key concepts in preparation for your presentations and final exam. Quizzes that are missed may be taken later with the instructor approval.

Team Exercise: Student teams will develop their security organization in a fictitious company, propose an annual budget, and design a new facility. A power point presentation of findings to the class is required.

Final Exam: The examination will be comprehensive and consist of a combination of essay and short answer questions to test your overall knowledge and understanding of the concepts and principles of corporate security management and operations**.**

Class Policies *Vary based on university requirements and instructor preference.*

SIS 410 Corporate Security Operations and Management **LESSON PLAN**

Week	**Topic Areas**	**Instructional Methods**	**Student Assignments**
1	**Course Introduction & Overview** • Historical Roots of Private Security	Classroom Presentation Class Discussion	Read Chapter 1 Visit ASIS International website
2	**Business Strategy , Leadership and Organization** • Outsourcing • Technical Knowledge • Strategy and Risk • Organizing activities • Establishing Objectives • Organizational Structures	Classroom Presentation and Discussion	Read Chapter 2,3,and 4
3	**Managing People** • Working through people • Maslow's theory • Staff development • Performance Evaluation • Employee Termination	Classroom Presentation and Discussion Quiz 1	Read Chapter 5
4	**Personnel Security and Training**	Classroom Presentation and Discussion	Read Chapter 14 , 18 & 21

	• Pre-employment Screening • Fair Credit Reporting Act • Cost benefit analysis • Drug testing • Employee security awareness training		
5	**Budget Development & Management** • Budget construction • Zero-based budgeting • Capital & Expense Budgets • Controlling Cost	Classroom Presentation and Discussion Team Project	Read Chapter 5
6	**Risk Management & Emergency Management** • Risk Analysis • Security review and Audit • Security Incident Causation Model • Emergency Operations Plan Business Continuity planning	Classroom presentation and discussion	Read Chapter 6 & 15
7	**Managing Guard Operations** • Legal issues • Selection and training • Proprietary vs. contract • Quality Assurance	Classroom presentation and discussion Model application Quiz 2	Read Chapter 7
8	**Managing Physical Security** • Safeguarding company facilities • Concentric protection • Detection, Intrusion, and Response • Lock and Key Systems		Read Chapter 8
9	**Mid- Term** • Review • Examination •	Classroom discussion	

10	**Managing Access Control** • Business Rationale • Types of ID and Access media • Access Control & physical Security • Closed-circuit television • Biometric devises	Classroom discussion	Read Chapter 9
11	**Managing Investigations** • Types of investigations • Investigative scopes and report writing • Crime scene and evidence collection • Forensic science application • Case management	Quiz 3	Read Chapter 13
12	**Workplace Violence** • Violence response Team • Policy • Liability • Security response		Read Chapter 20
13	**Team Projects** • Team Project Meetings • Team Project Presentations • Peer Review Sessions	Team Practical	
14	**Information Security** • Policies and procedures • Employee awareness • Paper and computer data • Competitive Intelligence		Read Chapter 17
15	**Terrorism Against the U.S.** • Threat Assessment • Weapons of Mass Destruction • Critical national infrastructure US • **Course Review**		Read Chapter 24.25,26,27 and 28
16	**Student Learning Assessment** Written Final Examination		

Course Number: CS 2XX **Credit Hours**: 3

Course Title: Network Administration

Required Texts:

1. Dye, McDonald, and Rufi, *Network Fundamentals, CCNA Exploration Companion Guide*, Cisco Press.
2. Halberg, Bruce. *Networking, A Beginner's Guide, Fifth Edition*. MaGraw-Hill

Course Description: The principles and practice of computer networking with emphasis on the Internet. The structure and components of computer networks are introduced including local area networks (LANS) and wide area networks (WANS); Methods of network installation and operations are introduced and practiced.

Goals: The student will learn the terminology describing the hardware and software components of computer networks. The student will use protocols, equipment, and topologies to understand various types of network systems. The student will learn and demonstrate skills in installing and administering network components.

Learning Outcomes:

1. Identify client/server and peer-to-peer networks.
2. Analyze and understand the network layering models.
3. Examine various networking protocols and standards.
4. Compare various networking media and topologies.
5. Identify Hardware and Software components of a typical LAN.
6. Identify Hardware and Software components of a typical WAN.
7. Construct and install components of a LAN.
8. Experiment with various networking utilities to determine the appropriate network support.

Student Assessment Activities

Assessment Item	Percentage of total score
Mid-Term Written Examination	25%
Software based Team Project	25%
Quiz 1	25%
Final Written Examination or Paper	25%
Total Assessment Score	100%

Class Policies *Vary based on university requirements and instructor preference.*

CS-2XX Network Administration Lesson Plan

Week	Topic Areas	Instructional Methods	Student Assignments
1	**Foundations:** • Binary numbers • measuring data	Classroom Presentation Class Discussion	
2	**Networking Fundamentals** • Network types: Peer to peer vs client/server • Network features: email, remote access, file sharing, internets and intranets • Network security • The OSI model architectures	Classroom Presentation Class Discussion	
3	**Cabling** • Cable topologies: • cable types: biaxial and twisted pair • cable installation: • SOHO networks		

4	**Network Hardware** • Directing traffic: repeaters, hubs, etc. • Gateways • Firewalls • Modems		
5	**WANs** • Determining needs • analyzing requirements • WAN connections		
6	**Protocols** • TCP/IP • Ports • Addressing • Other protocols		
7	**Directory Services** • Forests, Trees, Roots, and Leaves • NDS • Securing the scene		
8	**Directory Services Continued** • Active Directory • X.500 • LDAP		
9	**Remote Access** • Classifying remote users • Understanding access needs • Remote access technologies	Classroom discussion	
10	**Network Security** • Internal security • account security • External security • front & back door threats	Classroom discussion	
11	**Disaster Recovery** • Planning for disaster: scenarios, communications, offsite storage • Backup • Restore		

12	**Servers** • Server specifications • Choosing servers • Server maintenance		
13	**Client machines** • Desktop machines • Workstations • Peripherals		
14	**Installing Windows Server 2011** • Preparing for Installation • checking the configuration • Configuring server clients		
15	**Comprehensive Course Review**		
16	**Student Assessment** Comprehensive Final Examination or Research Paper		

Course Number: CS 3XX **Credit Hours**: 3

Course Title: Computer Forensics

Required Texts:

1. Computer Forensics: Investigating Network Intrusions and Cybercrime, EC-Council.
2. Guide to Computer Forensics and Investigations, Nelson/Phillips/Stewart
3. Computer Forensics Jump Start, Solomon, Barret, Broom
4. Digital Evidence and Computer Crime, 2nd Ed., Eoghan Casey.

Course Description: This course will introduce the necessary skills to identify an intruder‘s footprints and to properly gather the necessary evidence to prosecute. The basic methodologies and techniques of forensics will be discussed during this course. This course is for students interested in an overview of the knowledge and skills needed to identify, track, and prosecute the

cyber-criminal involving security inspection audit deficiencies and corrections, security violation investigations, and classified information loss or unauthorized disclosure.

Goals: After taking this course students should be able to discuss the acts which constitute types of computer crimes. They should understand the techniques used to detect and analyze various actions making up these types of acts**.** They should understand how these techniques comport with the law. They should be able to understand the relevant legal and ethical issues involving property and privacy. The last part of the course has students performing a mult-week exercise in which they must work in a team in order to first simulate a cybercrime. The second part of the exercise has the same teams attempting to solve a simulated cybercrime and then obtain sufficient evidence to convince the class that the original team committed that crime.

Learning Outcomes: Upon course completion, students will be able to:

1. Understanding cybercrime: hacking, IP theft,
2. Understand basics aspects of malicious software including viruses and worms
3. Be exposed to issues of cyber warfare, both historical examples and modern capabilities of state actors.
4. Understand issues of cyber terrorism, both examples and threats
5. Understand tracking cybercrime acts with permission, policies, logs, and signatures.
6. Be able to use modern software based tools of forensics: monitoring tools, software recovery, imaging, crackers, sniffers, intrusion detection.
7. Apply these tools in a realistic setting to detect, analyze and document a cybercrime.
8. Be able to use modern hardware based tools of forensics including hardware monitors
9. Preserving evidence: imaging, permissions and seals, validation and authentication.
10. Evidence Analysis: data classification, data reconstruction, forms of evidence.
11. Legal issues: reconstruction, fraud, privacy, case studies.

Student Assessment Activities

There will be weekly homework assignments that count for approximately 25% of the grade. There will be a midterm examination that counts for approximately 25% of the grade. There will also be a software based team exercise in forensics that counts for approximately 25% of the grade. Finally, there will be a final exam or a final paper that will make up the final 25% 0f the course grade.

Assessment Item	Percent of Total Grade
Weekly Homework	25%
Software –Based Team Exercise	25 %
Mid-term Examination	25 %
Final Written Examination or Paper	25%
Total Assessment Score	100 %

Class Policies *Vary based on university requirements and instructor preference.*

CS 3XX Computer Forensics Lesson Plan

Legend: Effective Security Management = **ESM**
Federal Information Security Manager = **FISM**

Week	Topic Areas	Instructional Methods	Student Assignments
1	**Actions warranting computer forensics** • Malicious software: hacking, malware, worms and viruses • Cybercrime: Intellectual property theft, child pornography, internet stalking. • Social networking and crime, the London riots, the Arab Spring,	Classroom Presentation Class Discussion	

	• Information warfare: Stuxnet, the Gulf war, the Russian invasion of Georgia		
2	**Hardware basics:** • Network architectures • Internet protocols • Computer components • Other devices	Classroom Presentation Class Discussion	
3	**Tracking techniques:** • Policies and permissions • System, application and device logs • Billing statements • Legal rights and employer/employee rights • Monitoring methods and procedures • Profiling		
4	**Software tools:** • Key loggers and system trackers • Data integrity checking • Password crackers • Sniffers	Classroom Presentation	
5	**Software tools continued** • Recovery and search software • Data wiping • Imaging tools • Encryption software	Class Discussion Practical Blueprint Reading Exercise Team Assignments	
6	**Hardware tools** • Cameras • Key logging devices • Recording devices • Intrusion detection/protection devices	Classroom presentation and discussion Fire Exit Controls Ingress & Egress Security Devices	
7	**Obtaining and preserving evidence** • Securing the scene	Discussion and review of technical requirements and	

	• Backing up original data, disc imaging • Securing evidence: public key encryption, token, permissions and seals • Validation and authentication • digital certificates and digital signatures	specifications of security systems and devices	
8	**Analyzing evidence** • Overview of different types of evidence • Guidelines • Classifying data • Reconstructing data	Classroom discussion Video	Student Exercise 4- Draft an emergency evacuation plan
9	**Legal issues** • Investigation procedures: search and seizure, corporate ethics • Crime reconstruction • Rule of evidence • Presentation of evidence	Classroom discussion	
10	School Break		
11	Class exercise I: Simulating cybercrime exercise 1 • Creating the scenario • Selecting the computer software program • Data input		
12	Class exercise I: Solving exercise 1 simulated crime • Tracking system intrusion • Collecting digital evidence • Identifying person(s)		

	responsible		
13	Class exercise II: Simulating cybercrime exercise 2 • Creating the scenario • Selecting the computer software program • Data input		
14	Class exercise III: Solving exercise simulated crime • Tracking system intrusion • Collecting digital evidence • Identifying person(s) responsible		
15	Comprehensive course review		
16	Student Learning Assessment • Written Final Examination Or Research paper		

Course Number: BA 308 **Credit Hours**: 3

Course Title: Public Administration

Required Texts:

1. Required: Starling, G. *Managing the Public Sector, 8th ed.*, Wadsworth, 2008.
2. Watson, R. *Public Administration: Cases in Managerial Role Playing*, Longman 2002.

Course Description: Public administrators and characteristics of public sector organizations are discussed. This course explores the impact of political processes and public pressures on administrative action, the role of regulatory agencies, and responsibilities of public administrators including human resource management, governmental budgeting, intergovernmental relations, and participation in the policy making process. Also discussed are

the qualifications of public administrator and the unique challenges faced by government officials.

Goals: This course is designed to provide insight into public administration, and the unique role of public administrators in society and organizations, including an understanding of responsibilities, limitations and challenges

Learning Outcomes:

1. Describe the historical and contemporary approaches to public administration and discuss the application to today‘s organizations with emphasis on managerial, legal, and political perspectives and pressures.
2. Compare and contrast the different levels of American government: local, state and federal, with relation to the role of public organizations and their functions. Explain the role of associated regulatory agencies, intergovernmental and community relations, and laws and regulations of interest to public administrators
3. Evaluate the growth and development of public and regulatory administration in the United States beginning with the creation of the Civil Service Commission in 1883, and appraise the effect of regulatory changes on contemporary business organizations.
4. Explain why public administrators must understand the constitutional values of separation of powers, legitimacy, diversity, liberty and freedom, property rights, procedural due process, equal protection, equity and justice, administrative accountability, ethics, and stewardship.
5. Compare public and private sector budgeting approaches and obligations, and discuss federal budget cycle timelines and processes. Also compare public and private sector approaches to planning, decision-making and collective bargaining.
6. Discuss the nature, historical development of the policy-making process. Explore current issues and public policies, and discuss the use of policy analysis and program evaluation to determine the success of a policy.
7. Discuss public program implementation including responsibilities associated with contracting, privatization, case management and threats to effective program implementation.
8. Discuss governmental personnel issues (human resource management), employee recruitment, evaluation, disciplinary procedures, labor laws, and the civil service system.
9. Engage in individual and team case analysis relating to several facets of public administration.

Course Information:

Case Studies Overview: Over the course of the semester, teams of 3-4 will engage in several in-class case analyses and one case presentation. Below is a *sampling* of possible cases:

- Dealing with Bureaucracy and Intergovernmental Relations: The EPA and Hazardous Waste
- Developing a New Policy: A Police Department Responds to Street Gangs
- Public Scrutiny and Accountability: An Ethical Dilemma in State Administration
- Dealing with Inmates and Image: A Prison Town‘s Dilemma
- Restoring Mystic Lake: Program Choices When Science is Ambiguous
- The Politics of County Budgeting: Piecing Together the Budget Puzzle

For the Case Assignments, each team will designate a ―scribe" to take notes for each case; this task will rotate. Consider this to be like a ―public hearing" on the issue at hand. The teams will discuss the case from the perspective of at least three stakeholders. The scribe will take notes, which will be used to create the team case brief containing the following sections.

- Case Intro – including a ―role-play" role
- Stakeholders (include the ―force field" of politics model)
- Problem Definition (blocked managerial objective)
- Analyze Causes (blockage or constraints).
- Develop and Evaluate Alternatives (include ―public hearing" comments)
- Select Solution (and explain choice relative to other alternatives)
- Recommend Detailed Plan of Action for Implementation – including the final policy, plan(s) and programs to be implemented.

Student Assessment

- Weekly Participation – Exercises and Team Case Participation 15%*
- Case Briefs(s) 30%
- Case Presentation 10%
- Key Terms Exams – 2 x 25% 50%
-

Assessment and Evaluation:

Assessment Items	**Percentage of Final Course Score**
Weekly participation	15 %
Case Briefs	30%
Case Presentation	10%

Key Terms Exams – 2 x 25%	50%
Total Assessment Score	100%

Class Policies *Vary based on university requirements and instructor preference.*

BA 308 Public administration Lesson Plan

Week	Topic Areas	Instructional Methods	Student Assignments
1	**Course Introduction** What is Public Administration? Who is involved in it?	*State of Union* Video Classroom Presentation Class Discussion	Chapter 1
2	**Public Policy**	*Economic Meltdown*	Chapter 2
3	**Intergovernmental Relations**	EPA/Hazardous Waste Case Study	Chapter 3
4	**Admin Responsibilities and Ethics**	Ethical Dilemma Case Study	Chapter 4
5	**Planning/DM**	Police and Gangs case Study	Chapters 5 & 6
6	**Key Terms Exam I**		Chapters 1-6
7	**Organizing**		Chapter 7
8	**Leading**	Leadership Video	Chapter 8
9	**Spring or Fall Break – No Classes**		

10	**Implementation and Evaluation**	Inmates and Image case Study	Chapter 9
11	**Implementation and Evaluation**	Mystic lake Case Study	Chapter 9
12	**Human Resources**	Guest Speaker- HR Manager	Chapter 10
13	**Human Resources**	Star Award Example	Chapter 10
14	**Case Presentations**		
15	**Public Budgeting**	Budget Example	Chapter 11
16	**Student Learning Assessment Key Terms Exam II,**		Chapters 7-11

Course Number: BA 4XX **Credit Hours**: 3

Course Title: Government Acquisitions and Contracting

Prerequisite: BA 201- Principles of Management

Required Texts:

1. Federal Acquisition Regulations (FARS)
2. Department of Defense Regulation Supplements (DFARS)

Handouts, definitions and case studies from a variety of additional texts to be provided by the professor.

Course Description: This course will provide an analysis of Government contracting regulations and contract administration/management procedures, with particular emphasis on the Federal Acquisition Regulation (FAR) and the Department of Defense Regulation Supplement

(DFARS), and the practical application of the FAR and DFARS in Government and industry contract administration/management roles.

Goals: Upon completion of this course, the student should have good understanding of the government acquisition, contract administration and management policies, procedures and regulations. The student will be familiar with the roles of the contract officer, contract officer‘s technical representative and the program security management.

Learning Outcomes: Upon course completion, students will be able to:

1. Discuss the basis framework of the Federal acquisition environment.
2. Identify the basic principles of federal government contracting.
3. Locate, cite, interpret and/or utilize information in the FAR and DFARS that is applicable to government acquisitions.
4. Identify the major elements of acquisition planning.
5. Explain the policies pertaining to required and preferred sources of supplies and services.
6. Determine the appropriate method of contracting (and contract type) for a given contracting scenario, and if a special contracting method would be appropriate.
7. Apply the pre-solicitation requirements of the various socioeconomic programs for a given contracting scenario.
8. Understand and utilize the policies and procedures associated with procurement planning.
9. Discuss the requirements and process for properly publicizing contract opportunities.
10. Identify the policies and procedures governing competitive and noncompetitive negotiated acquisitions, sealed bidding, and contractor qualifications.
11. Explain the policies and procedures for processing simplified acquisitions, using special negotiation procedures and pricing negotiated contracts.
12. Discuss the policies and procedures for contract preparation and processing contract modifications.
13. Identify the rights of the parties when contract performance is not timely or does not comply with contract specifications.
14. Describe the rights and process for complete or partial termination of contracts for the convenience of the Government or for default.
15. Identify requirements of the applicable contract clause to a given contracting scenario.

16. Determine the amounts payable to the contractor in accordance with the applicable payment clauses for a given contracting scenario.

17. Identify the policies and procedures for filing protests, and for processing contract disputes and appeals.

18. Explain the policies and procedures for closeout of contract files.

19. Demonstrate an understanding of the ~~l~~language" of the federal budget including identification of budget process stages, and factors that influence the budgeting process.

20. Discuss the impact of public sector budget rules (and schedules) on policy and acquisition decisions.

21. Convey an understanding of the employer-employee relationship in government and industry including personnel policies and methods; selection, placement, training and promotion of employees; and recent trends in employment practices.

22. Discuss the business development process, including security's role in that process.

Student Assessment Activities

Individual Experiential Learning Exercises (15) @ 50 each	750
Final Written Examination	250
Total Assessment Score	1000

Student Scoring & Grade Matrix

1000-900	A	Superior
899-800	B	Above Average
799-700	C	Average
699-600	D	Below Average
600 and below	F	Failure

Description of Assessment Activities

Experiential Learning Exercises 1-15.

The Experiential Learning Exercises are case studies or simulations where the student will take the information learned in the presentation stage and create a finished product to show comprehension of the material.

Final Exam: The examination will assess the student's comprehensive knowledge and understanding of Government Acquisitions and Contracting. The written test will consist of a combination of essay questions and practical scenarios to evaluate the student's overall knowledge and their ability to apply the knowledge in real-world scenarios.

Class Policies *Vary based on university requirements and instructor preference.*

SIS 4XX Government Acquisitions and Contracting Lesson Plan

Week	Topic Areas	Instructional Methods	Student Assignments
1	Framework & Basic principles of Federal Government Contracting • Definitions • Terms • Process overview • FAR-Online overview	• Classroom Presentation • Class Discussion • FAR-Online video	Read FARs & DFARS Experiential Learning Exercise # 1
2	FAR & DFARS • Locate • Site • Interpret • Utilize Information • Identify Major Elements	• Classroom Presentation • Class Discussion • Video • Example of Experiential Learning Exercise	Read FARs & DFARS Experiential Learning Exercise # 2
3	Policies • Required & Preferred Sources • Suppliers verses Services • Appropriate Extent of Competition	• Classroom Presentation • Class Discussion • Video • Example of Experiential	Read FARs & DFARS Experiential Learning Exercise # 3

		Learning Exercise	
4	Contracting • Type/Method • Special methods • Pre-solicitation Requirements of socioeconomic programs	• Classroom Presentation • Class Discussion • Video • Example of Experiential Learning Exercise	Read FARs & DFARS Experiential Learning Exercise # 4
5	Procurement Planning • Policies • Procedures • Proper Publicizing	• Classroom Presentation • Class Discussion • Video • Example of Experiential Learning Exercise	Read FARs & DFARS Experiential Learning Exercise # 5
6	Policies/Procedures • Competitive & noncompetitive • Sealed Bidding • Contractor Qualifications • Simple Acquisition Pricing Negotiated Contracts	• Classroom Presentation • Class Discussion • Video • Example of Experiential Learning Exercise	Read FARs & DFARS Experiential Learning Exercise # 6
7	Policies/Procedures • Contract Preparation • Processing Contract Modifications • Contract non-Performance • Termination	• Classroom Presentation • Class Discussion • Video • Example of Experiential Learning Exercise	Read FARs & DFARS Experiential Learning Exercise # 7

8	Policies/Procedures • Filing Protests • Processing Contract Disputes & Appeals	• Classroom Presentation • Class Discussion • Video • Example of Experiential Learning Exercise	Read FARs & DFARS Experiential Learning Exercise # 8
9	Policies/Procedures • Closing out Contract Requirements	• Classroom Presentation • Class Discussion • Video • Example of Experiential Learning	Read FARs & DFARS Experiential Learning Exercise # 9
10	Payment Clause • Determining Amount Payable for applicable scenario	• Classroom Presentation • Class Discussion • Video • Example of Experiential Learning Exercise	Read FARs & DFARS Experiential Learning Exercise # 10
11	Public Sector Budgets • Process Stages • Rules • Schedules • Impact on Policy and Acquisition Decisions	• Classroom Presentation • Class Discussion • Video • Example of Experiential Learning Exercise	Read FARs & DFARS Experiential Learning Exercise # 11
12	Corporate Financial Management • Concepts • Public versus Private Sector • Impact of Mandates	• Classroom Presentation • Class Discussion • Video • Example of Experiential Learning Exercise	Read Handouts Experiential Learning Exercise # 12

13	Strategic Planning Process • Internal Audits • External Audits • Establish Objectives • Evaluate and Select Strategies	• Classroom Presentation • Class Discussion • Video • Example of Experiential Learning Exercise	Read Handouts Experiential Learning Exercise # 13
14	Employer –Employee Relationships • Employment trends • Personnel policies • Staffing • Compensation • Labor Unions and bargaining Legal Considerations (EEOC & Affirmative Action)	• Classroom Presentation • Class Discussion • Video • Example of Experiential Learning Exercise	Read Handouts Experiential Learning Exercise # 14
15	Business Process Development • Defining current state of Processes • Identifying Gaps & Opportunities • Designing Future Processes	• Classroom Presentation • Class Discussion • Video • Example of Experiential Learning Exercise	Read Handouts Experiential Learning Exercise # 15
16	Course Review & Student Learning Assessment Comprehensive Course Review Written Final Examination	Comprehensive oral review of the course's learning objectives and main topics.	Final test

Course Number: SIS 430 Credit Hours: 3

Course Title: Introduction to Emergency Management

Required Texts:

1. George D. Haddon & Jane A. Bullock, Introduction to Emergency Management, 3rd Edition, Elsevier Butterworth-Heinemann, Burlington, MA 2008

2. Supplemental readings provided to students in this class

Course Description: This course provides students with a comprehensive overview of national and state emergency management practices within the United States. This course will familiarize the students with the basic concepts and principles of the emergency management discipline. The course will focus on planning and leadership during emergency preparedness and mitigation activities, emergency response, emergency recovery and emergency communications. During the course, the students will discuss the individual roles of the federal and state governments and the importance of coordinating their efforts in any emergency event. The students will also be familiarized the National Response Framework and the National Incident Management System and their application during both natural and manmade emergencies. Students will also review and discuss business continuity planning and plans.

Goals: This course is one of the six main courses in the Criminal Justice and Security Area of Concentration in the Global Security &Intelligence Program. While not required for any program of study, this course may be an approved substitution in the ABA or AS programs as with the respective program manager‘s approval. Upon completion of SIS 495, the student will be equipped with the knowledge and analytical skills necessary to understand and participate in emergency management activities as a private citizen, government official or business manager. The student will also be familiar with the discipline of emergency management and its applications in both in the government and private sectors. Finally, the student will be familiar the Federal Emergency Management Agency (FEMA); the National Response Framework and the National Incident Management System.

Learning Outcomes:

1. Demonstrate a general knowledge of the historical development of emergency management within the United States.

2. Understand the organization and mission of the U.S. Department of Homeland Security (DHS) and the Federal Emergency Management Agency (FEMA)

3. Understand the roles and interdependency of federal, state and local governments in responding to and mitigating both natural and manmade disasters.

4. Understand the principles of business emergency and continuity planning

5. Demonstrate the capacity to use analytical methodologies to identify hazards, prioritize hazards and to suggest appropriate mitigation strategies

6. Be able to draft an emergency action plan for a specific disaster

7. Effectively critique and participate in citizen and government discussions of emergency management issues

8. Be familiar with the National Response Framework & the National Incident Management System

9. Learn how to use the Federal Emergency Management Agency's on line training programs.

10. Produce professional (individual and group) quality reports and presentations.

Scoring and Grading Matrix

Points	Grading Elements:
100	2 Quizzes
100	Team Planning Exercise & Presentation
75	Complete 3 FEMA On-Line Courses
25	Individual Research Paper
100	Table Top Exercise
100	Final Examination
400 points	Total Course Points Available

Description of Assessment Activities:

Quizzes: There will be based on readings and class lectures. They are intended to help you understand the reading and key concepts in preparation for your presentations and final exam. Quizzes that are missed due to an excused absence may be taken later with the instructor approval.

Team Planning Exercise: Student teams will identify and research hazards (manmade or natural) in particular geographic area, conduct an area vulnerability assessment, and present their findings in a power point to the class.

FEMA Courses: This course requires that the student enroll in FEMA's Independent Study Virtual Campus and complete the three assigned courses. The student must submit a course completion certificate evidencing their successful completion of the assigned courses as scheduled to the instructor**.**

Team Table Top Exercise: Your team will participate in a table top emergency response exercise using Incident Commander, a computer simulation game, to demonstrate your familiarity with the Incident Command System and its operation. Your team will be evaluated on their preparedness for the exercise and effectiveness during the exercise.

Individual Paper: The term paper will focus on a specific disaster evaluating the preparedness and response of local state and federal agencies. The term paper shall be a minimum of 8 pages with at least 6 references. Authoritative, reliable references are required. Use the APA format in developing your paper and citing references.

Final Exam: The examination will be comprehensive and consist of a combination of essay and short answer questions to test your overall knowledge and understanding of the concepts and principles of emergency management and their application during emergency events.

Class Activities:

Class Policies: Vary with institution and instructor preference

SIS 430 Introduction to Emergency Management Lesson Plan

Week	Topic Areas	Instructional Methods	Student Assignments
1.	**Emergency Management** • Course introduction and overview • Definition • History of Emergency Management in US • Career Opportunities & education	Classroom Presentation Class Discussion FEMA Video	Chapter 1
2.	Natural & Technological Hazards –Overview • Concept of Risk Mgmt. • Natural and manmade		Chapter 2
3.	**Risk Management** • Concepts • General Approaches to Risk Management • Threat Identification • Natural and Manmade		
4.	• Hazard ID & Mitigation • Types of Hazards • Types of mitigation	Quiz 1	Chapter 3
5.	**Emergency Preparedness** Threat Levels • Vulnerability factors • Criticality • Threat Assessment Matrix		Chapter 6
6.	**Emergency Response**	Classroom presentation and discussion Field Trip to AZ EOC	Chapter 4

7.	**National Response Framework** • Purpose • Core Concepts • Components • Federal, State and local government roles • Private and NG Organizations roles	Classroom presentation and discussion	Read Handouts Visit NRF Website FEMA Website
8.	**NIMS & Incident Command System ICS –** • ICS system • ICS roles • NIMS and ICS • Key concepts review	Classroom Presentation and Discussion	FEMA Handouts
9.	**Review & Examination** • Basic EM Concepts & Applications • Post Examination Review	Classroom discussion Quiz 2	3 FEMA Courses Due
10.	**Disaster Recovery** • FEMA‘s role	Classroom discussion	Chapter 5
11.	**International Disaster Management Emergency**		Chapter 8
12.	**Hurricane Katrina Case Study**	View videos Discuss mistakes Panel discussion of the event	Handouts & Read Pages 397-444 Videos
13.	**Team Permutations** • Team Project Presentations • Peer Review Sessions		
14.	**Incident Commander Training** • Guest Speaker	Learn to use FEM training software Incident Commander	Read Handout

15.	**Class Table Top Conducted** • Using Incident Commander • Teams • Comprehensive Course Review		
16.	**Student Learning Assessment** Written Final Examination		

Course Number: SIS 420 **Credit Hours:** 3

Course Title: Aviation Security and Technologies

Required Texts:

1. Price & Forrest, Practical Aviation Security, Elsevier, Boston, MA, 2009
2. Current TSA Regulations as required, free download from TSA Website

Course Description: This course is designed to provide the student with a comprehensive overview of aviation security including both air carrier and airport security as well as provide students with substantive research opportunities in aviation security. The students will also be familiar with the Transportation Security Administration regulations (49CFR 1500 series) and how they apply to airport, aircraft operator, and indirect air carrier operations and security programs. This course will concentrate on the disciplines of security and intelligence as applied to aviation. Students will learn to apply the four core security disciplines: communication security, operations security, physical security, and personnel security in the aviation sector. Of prime concern in this course is aviation sector‘s readiness to prevent and respond to the following threats: hijackings, bombings, missiles, and shootings, CBRN attacks perpetrated by terrorists and others with non-political criminal intent. The course will focus on the preventive security measures taken and proposed by airports, the air carriers, and the U.S. Transportation Security Administration. Of secondary concern is criminal behavior by airport and airline personnel with aviation security impact as well as civil liberty issues associated with security screening. Students may engage in aviation security legislation and policy review, undertake substantive aviation security-related research, generate recommendations to improve air carrier and airport security, and evaluate emerging technologies. Some students may volunteer for participation in an on-site security review at a major international airport.

Goals: Students will gain a comprehensive understanding of civil aviation security including both air carrier and airport security. The students become familiar with the Transportation Security Administration regulations (49CFR 1500 series) and their practical application in airport, aircraft operator, and indirect air carrier operations.

Learning Outcomes:

1. Understand the basic concepts of aviation security and their application to commercial aircraft operators, airports, freight forwarders, and general aviation.

2. Understand aviation threats including aircraft hijackings, bombings, and on-board shooting, airport bombings and attacks as perpetrated by terrorists, individuals with non-political motives, and emotionally disturbed individuals.

3. Understand the insider-threat posed by airline or airport personnel who engage in criminal behavior and the impact that the threat poses to aviation security.

4. Understand the regulatory roles of government agencies and the relevant aviation security laws and regulations.

5. Be familiar with aviation security issues impacting commercial air service, air cargo and general aviation operations.

6. Be able to perform an elementary, security risk management assessment of air carrier and airport operations.

7. Be familiar with the variety of security measures and types of security equipment used for securing aircraft and airports.

8. Grasp the importance of and need for use of biometrics and other emerging technologies in airport and air carrier security.

9. Produce professional (individual and group) quality reports and presentations.

Description of Assessment Activities:

Points	Grading Elements:
100	Mid-Term Examination
100	Team Exercise & Presentation
50	Individual Knowledge Application Exercises
50	Individual Research Paper
100	Final Examination
400 points	Total Course Points Available

Mid-Term Exam: The examination will combine both survey and essay type questions to test your overall knowledge and understanding of aviation security concepts and applications discussed in the course to date. .

Team Exercise & Presentation: Develop either an airport or aircraft operator security program using current Transportation Security Regulations as a guide. The team will be task with writing various security policies and procedures for their airport or aircraft operators. Teams will be evaluated on the thoroughness of their proposed security programs, the clarity and quality of their assigned policies and procedures and compliance with the relevant TSA regulations. Their presentation must provide a general overview of their chosen aviation operation, a review the of the applicable TSA regulations, details of their proposed security plan, and a discussion of the security policies and procedures that they wrote. Presentations should last 15-20 minutes. Students are to wear business attire. The team will present their findings to the class using Power Point. The use of graphics, video clips, photographs, or props to support your presentation are encouraged. At the conclusion of your presentation, you must provide a copy of your presentation including a bibliography identifying the sources that you used in developing your presentation. Team presentation evaluation will include quality of the presentation, supporting research, team member participation, professional manner and dress. Peer evaluations will be included in the overall evaluation. All team members will receive the same score unless they have not significantly participated in the research effort or the presentation as determined by their team mates and the instructor.

Individual Research Paper: The term paper will focus on a specific security problem or issue. The term paper shall be a minimum of be 5 pages not including title or reference pages with at least 6 references. Authoritative, reliable references are required. Use the APA format in developing your paper and citing references. No late papers will be accepted

Individual Knowledge Application Exercises - These are practical scenarios that require the individual to apply his or her aviation security knowledge in practical scenarios. Each scenario is worth 10 points.

Final Exam: The exam will be a combination of essays and short answer questions to test your overall knowledge and understanding of the concepts and principles of aviation security and their application in practice

Class Policies: Vary with college or university and instructor preference

Class Activities:

SIS 420 Aviation Security and Technologies Lesson Plan

Week	Topic Areas	Instructional Methods	Student Assignments
1.	**Aviation Security** • Course introduction and overview • Aviation Operations Overview • Career Opportunities & education	Classroom Presentation Class Discussion	Chapter 1 and 2
2.	**Role of Government in Aviation Security** • Defining the role of the TSA and FAA • The role private and public stakeholder • Review of 49 CFR 1500 Regulations		Visit TSA Website and review general format and availability of TSA regulations r
3.	**Threats to Civil Aviation** • Historical threats • Hijacking • Bombing		Chapter 2
4.	Regulatory Review and Discussion • Sensitive Security Information-49CFR 1520 • Civil Aviation Security: General Rules 49CFR1540	Review and discuss of both regulations and their meaning	Download each regulation from TSA Website
5.	Airport Security Practice and Regulations • 49CFR 1542 • Airport Security Programs • Airport Security Coordinator • Airport Security Areas • Criminal History Records Checks • Challenge Procedures	Class Review and Discussion Practical Application Scenarios	Read Chapter 5 Read 49CFR 1542

6.	Airport Access Control & Physical Security Measures • Secure, SIDA, and AOA areas • Access controls	Classroom presentation and discussion	
7.	**Aircraft Operators Security** • 49CFR1544 Regulation • Aircraft Operator Security Coordinator • Inflight Security Coordinator • Ground Security Coordinator • Aircraft Operator Standard Security Program (AOSSP)	Class Review and Discussion Practical Application Scenarios	Read 49CFR 1544 Chapter 8
8.	**Mid- Term Review & Examination** • **A**viation Security Concepts & Applications • Post Examination Review	Written Examination	
9.	**Passenger & Baggage Screening & Equipment** • Passenger Security Screening Concepts & Applications • Screening Equipment Technologies • Civil rights and other legal issues	Classroom discussion	Chapter 6-7
10.	**Air Cargo Security** • AOSSP cargo requirements • Indirect Air Carriers • Containerized vs., bulk • Screening technologies and equipment	Classroom presentation and discussion	Read Chapter11 49CFR1544 49CFR1548 49CFR1550
11.	**TSA Inspections & Enforcement** • TSA Inspector‘s Authority • Types of Violations • Penalty Assessment	Classroom review and discussion Practical enforcement scenarios	Download TSA Enforcement Guidelines

12.	**International Civil Aviation Organization** • ICAO Organization • Annex 17 Security Standards • Recommendations vs. standards • Enforcement mechanisms	Instructor presentation and discussions	
13.	**General Aviation Airport Security** • Airport Watch Program • Alien Flight Training Program • TSA Security Guidelines	Classroom Presentation Video General aviation airport threat assessment	Read Chapters 9-10
14.	University Holidays		
15.	**Team Presentations**		
16.	**Course Review & Student Learning Assessment** Comprehensive Course Review Written Final Examination		

This Page Intentionally Left Blank